OSAC Technical Series 0002

A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence

OSAC Task Group on Digital/Multimedia Science

http://dx.doi.org/10.29325/OSAC.TS.0002

OSAC Technical Series 0002

A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence

Prepared for
The Organization of Scientific Area Committees for Forensic Science (OSAC)

By
Mark Pollitt
Eoghan Casey
David-Olivier Jaquet-Chiffelle
Pavel Gladyshev
OSAC Task Group on Digital/Multimedia Science

January 2018

http://dx.doi.org/10.29325/OSAC.TS.0002

Abstract

Like many other specializations within forensic science, the digital/multimedia discipline has been challenged with respect to demonstrating that the processes, activities, and techniques used are sufficiently *scientific*.[1] To address this issue, in April 2015, the Organization of Scientific Area Committees for Forensic Science (OSAC) Digital/Multimedia Scientific Area Committee (SAC) established a Task Group (TG). This document summarizes the work of the TG that grew into establishing a harmonizing framework for forensic science practices and digital/multimedia evidence.

The TG researched and deliberated on the essential elements of digital/multimedia science, the nature of evidence examined, the overarching scientific principles and reasoning processes, the questions addressed by core forensic processes, and the activities and techniques which support the core forensic processes. It reviewed a large volume of pertinent literature, conducted interviews of practitioners, academics, and other interested parties.

Over a three-year period and many hours of debate, more than 40 discussion drafts were produced. The TG determined that digital/multimedia evidence, and other forensic disciplines, would be in a much stronger position to demonstrate their scientific basis as a harmonized forensic science rather than as mere disciplines at the intersection of forensic specialties and other sciences. **The value of forensic science as a whole is that it uses scientific reasoning and processes within the framework articulated in this document to address questions – specific to an event or a case – for legal contexts, to provide decision-makers with trustworthy understanding of the traces in order to help them make decisions**. The TG considered how the definitions and framework developed in the context of digital/multimedia evidence mesh with forensic science as a whole.

The present document describes the concept of traces as the core nature of forensic evidence and the fundamental object of study in forensic science. It proposes a broad definition of forensic science, not limited to legal problems in civil and criminal justice systems (courtroom contexts), and describes the different types of reasoning that play a significant role in forensic science. Then it defines five core forensic processes, seven forensic activities, and three operational techniques. The formalization of forensic science reasoning processes and outcomes in this work leads to increased reliability, repeatability, and validation in forensic results. This, in turn, gives decision-makers increased confidence in and understanding of forensic results.

The resulting definitions and framework can be used to harmonize concepts and practices within digital/multimedia science, and are likely applicable to most forensic disciplines. As such, this work may be useful in articulating their scientific basis, and promoting forensic science as one science, which is more than the union of a patchwork of forensic disciplines. The new paradigm created by the digital realm brings a unique opportunity to revisit fundamental definitions in forensic science and to strengthen the identity of forensic science as a whole, unified by common principles and processes that can address questions for legal contexts.

[1] The scientific basis of forensic science as commonly practiced has been widely questioned (Kennedy, 2003)

This document represents the conclusions and recommendations of the TG as of the date of its writing. The work continues and future versions of this document can be expected to contain new observations and updated conclusions.

Table of Contents

1. Executive Summary

In April 2015, the Organization of Scientific Area Committees for Forensic Science (OSAC) Digital/Multimedia Scientific Area Committee (SAC) established a Task Group (TG) to clarify how digital/multimedia fits within forensic science, and what questions are addressed using digital/multimedia evidence. The TG was composed of academics and practitioners, including international representatives. The TG conducted surveys, and solicited feedback from within the OSAC and from international partners to refine the understanding of digital/multimedia science as a forensic discipline, and of forensic science itself.

In practice, digital/multimedia evidence serves investigative, procedural, and scientific functions, and the outcomes of these multiple modalities are synthesized into expert opinions and conclusions. To clarify which aspects of this domain are scientific, this document concentrates on specific forensic questions that can be addressed by the systematic and coherent study of digital/multimedia traces.

The TG reviewed a great deal of literature concerning the kinds of questions that forensic science deals with and attempts to answer. This effort enabled a definition of forensic science as one science, unified by common principles and processes, rather than a patchwork of disciplines and activities. In addition, this effort led to a set of questions that forensic science addresses, and formalized a framework of scientific reasoning used to address these forensic questions. This framework instantiates the foundational notion that science is the systematic and coherent study of phenomena.

The TG developed generalized definitions for core forensic processes, and applied these definitions to digital/multimedia evidence. These definitions form a coherent set of intertwined definitions. These unifying concepts will make the communication and interchange between the disciplines much more effective for practitioners and for all external customers of forensic science. Such harmonization of understanding strengthens the identity of forensic science as one science, unified by common principles and processes that can address questions for legal contexts including, but not restricted to, problems that do not have prior probabilities or well-established knowledge.

In summary, this work posits that the various disciplines of forensic science have the following commonality:

They address forensic questions using similar methods and a series of activities that apply operational techniques and core forensic processes to traces.

To avoid confusion caused by inconsistent terminology across forensic disciplines, it is especially important to separate the labels naming the core forensic processes from the terminology used by different forensic disciplines to describe their processes, results and conclusions. To clarify this distinction, Appendix 1 categorizes a selection of questions that forensic scientists are asked to address. Appendix 2 provides examples of operational techniques that do not directly address specific forensic questions, but provide the necessary information for the forensic activities or to address forensic questions.

2. Forensic Science

A definition of forensic science should focus on the evidence scrutinized and the questions answered by the inquiry. After extensive research, surveys, and discussions, the TG formed the following understanding of the aim and purpose of forensic science:

The term forensic is defined as "relating to or dealing with the application of scientific knowledge to legal problems" (Merriam-Webster). This includes investigative activities performed in support of legal problems, as well as development of testimony for use in courts of law.

Traces are the *fundamental objects of study* in forensic science. A trace is a vestige, left from a past event or activity, criminal or not. The principle that every contact leaves a trace was initially attributed to Edmond Locard, and has evolved into a new definition of the trace to include a lacuna in available evidence, as well as activities in virtual settings (Jaquet-Chiffelle, 2013):

A trace is any modification, subsequently observable, resulting from an event.

This is not to suggest that all forensic questions involve event reconstruction, merely that all traces involve some modification. Even immutable objects can be a trace when their occurrence in relation to a forensic inquiry is the consequence of an event (e.g., a mobile device identifier deposited at a crime scene, or DNA transferred onto a victim). The modification can affect an entity in an environment or the environment itself. Its nature can be physical or virtual, material or immaterial, analog or digital. It can reveal itself as a presence or as an absence.

Forensic science addresses questions, potentially across all forensic disciplines. These questions are addressed using a specific and finite number of core forensic processes. For the purpose of this document, these processes are labeled as: 1) authentication, 2) identification, 3) classification, 4) reconstruction, and 5) evaluation.

The following definition of forensic science emerged from this work:

The systematic and coherent study of traces to address questions of authentication, identification, classification, reconstruction, and evaluation for a legal context.

The term *systematic* in this definition encompasses empirically supported research, controlled experiments, and repeatable procedures applied to traces. The term *coherent* entails logical reasoning and methodology. This definition uses legal context in the broadest terms, including the typical criminal, civil, and regulatory functions of the legal system, as well as its extensions such as human rights, employment, natural disasters, security matters.

3. Digital/Multimedia Evidence

To understand the scientific foundations of digital/multimedia evidence and how this fits into forensic science, it is necessary to consider the specializations of digital/multimedia evidence. Digital/multimedia evidence encompasses the following sub-disciplines, which are organized according to the current OSAC structure:

Speaker recognition: handling voice recordings in analog or digital form, including comparison of voice recordings with a known speaker for forensic purposes, comparison of voice recordings of unknown speakers, counting the number of speakers on a voice recording, and segmenting a voice recording into segments by speaker ("diarization"). In addition, principles developed for testing the performance of speaker recognition software have evolved into an international standard for all biometric modalities and applications (ISO/IEC 19795-1).

Facial identification: handling photographs and videos containing an unknown face for comparison with facial images in a database, or with a known subject for forensic identification purposes. Facial identification methods have been validated through empirical studies and found to be accurate (White et al, 2015).

Video/image technology and analysis: handling images and videos for forensic purposes. This includes classification and identification of items, such as comparing an item in an image or video with a known item (e.g., car, jacket). This also includes authentication of images and videos, metadata analysis, Photo Response Non-Uniformity (PRNU) analysis, image quality assessment, and detection of manipulation. Operational techniques include image and video enhancement and restoration.

Digital evidence: handling digital traces for forensic purposes, including classification and identification of items, activity reconstruction, detection of manipulation (e.g., authentication of digital document, concealment of evidence). Within the current OSAC structure, audio recordings are treated as a form of digital evidence for enhancement and authentication purposes.

The foundational sciences for the various sub-disciplines of digital/multimedia evidence are primarily biology, physics, and mathematics, but also include: computer science, computer engineering, image science, video and television engineering, acoustics, linguistics, anthropology, statistics, and data science. Principles of these, and other disciplines, are applied to the traces, data, and systems examined by forensic scientists. Study of foundational principles in digital/multimedia evidence is ongoing, with consideration for their suitability in forensic science applications.

Furthermore, many digital traces are changes to the state of a computer system resulting from user actions. In this context, the discovery of principles in how computer systems function, is a fundamental scientific aspect of digital/multimedia evidence. The systematic and coherent study of digital/multimedia evidence is made more complicated by the evolving nature of technology and its use. While the foundations of digital/multimedia evidence are largely in computer science, computer engineering, image science, video and television engineering, and data science, the underlying digital traces are, in large part, created by actions of operating systems, programs, and hardware that are under constant development. As a result, it will not always be possible to test in advance the performance of such systems under every possible combination of variables that may arise in casework. However, it may be possible, to test the performance of a particular system under a particular set of variables in order to address questions arising in a specific case. For instance, digital documents created using a

new version of word processing software can exhibit digital traces that were not previously known. The observed traces can be understood by conducting experiments; studying the software under controlled conditions. In this manner, generalized knowledge of digital/multimedia evidence is established and can be used by any forensic scientists to obtain reproducible, widely accepted results.

4. Non-technical Sources of Error

Error mitigation is an important consideration for digital/multimedia evidence (SWGDE, 2017). Even when all operational techniques are working perfectly, there is the potential for cognitive bias and other non-technical sources of error to skew forensic results.

There are multiple non-technical causes of errors involving digital/multimedia evidence (Sunde, 2017). Lack of competence can result in errors in forensic results, including overlooked and misinterpreted traces. Forensic laboratory management can also contribute to errors by using performance metrics based on speed over quality of results. Cognitive bias and observer effects are well-established problems in forensic science (Risinger et al, 2002). Even experienced forensic scientist are susceptible to cognitive bias such as concentrating on confirming a particular hypothesis, generalizing from small sample size, ease of retrieving an analogous example, and the degree of similarity with the observer's conception (Tversky & Kahneman, 1974). In actuality, higher expertise can make a person more susceptible to cognitive bias and contextual influences (Dror, 2011).

In some circumstances, it is necessary to have a forensic scientist provide expertise in the investigative phase in order to recognize potential sources of evidence and handle them properly. In other circumstances, it is necessary to have a forensic scientist separated from the investigative phase (e.g., blinding or sequential unmasking) to reduce the risk of cognitive bias.

The fallibility of human reasoning provides strong motivation for following a scientific approach when analyzing digital/multimedia evidence in a forensic context. Although scientific practices cannot eliminate error, it is a necessary part of the strategy to mitigate these risks. An effective way to minimize bias, while providing transparency of the process is to follow a documented methodology.

5. Reasoning Processes in Forensic Science

To be scientific, a discipline must employ scientific reasoning. This raises the question, what reasoning processes does forensic science follow?

The scientific method can be described in terms of abductive, deductive, and inductive reasoning, sometimes referred to as the hypothetico-deductive model. Abductive reasoning eliminates implausible explanations and retains the most plausible explanation for (limited) available facts and traces, drawing analogies from past experience.[2] Deductive reasoning

[2] The term *abductive* was originally used by Peirce (Eco & Sebeok, 1983), and has more recently been described as *inference to the best explanation* (Lipton, 2004). However, to equate abductive reasoning with intuition neglects the significance of an experienced individual critically evaluating observable facts. The original term abductive is used here for compatibility with deductive and inductive terminology.

tests this most plausible explanation against observable traces, possibly through further study of facts, with particular scrutiny for contradictory facts (falsification). If any contradictory traces are found, the most plausible explanation must be revised. Inductive reasoning can lead to knowledge specific to an event or a case, providing decision-makers with trustworthy understanding of the traces to help them make decisions. Inductive reasoning can also lead to a theory generalized from multiple cases or from repeatable experiments, providing newly-established knowledge in forensic science.

Peirce initially described the relationships and distinctions between these three modes of reasoning, which can be modeled as a triangle (Eco & Sebeok, 1983). Margot, then Crispino, and Ribaux translated this triangle model into the context of forensic science which is adapted, illustrated, and annotated in Fig. 1. The sides of the triangles, depicted using dashed lines in Fig. 1, represent an ideal of full information or knowledge, which is rarely attainable. Each mode of reasoning combines two kinds of information or knowledge (input), as depicted in Fig. 1 by the arrows originating from two vertices and merging into the third (output). The gray shaded area represents the combination of two kinds of information or knowledge for each type of reasoning.

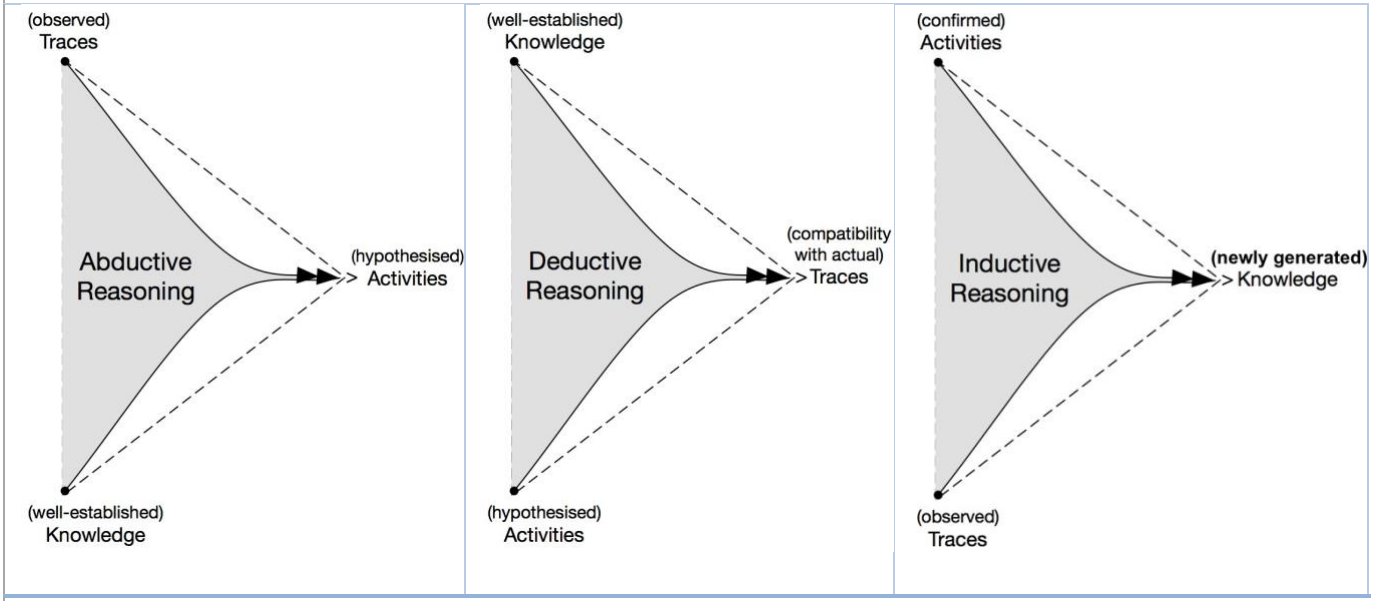

Figure 1: Depiction of abductive, deductive, and inductive reasoning in the context of forensic science, adapted from Ribaux (2014), Crispino (2008), and originally, Margot (2003).

This scientific reasoning process can be applied to all phases of a legal proceedings, from the initial investigation to the final decision, as well as research and experimentation. Whether establishing generalized theories, performing investigations, or evaluating specific traces, forensic scientists follow a cyclical process of abductive, deductive, and inductive reasoning. These modes of reasoning apply to forensic research, investigation, and evaluation as shown in Table 1.

Context	Abductive	Deductive	Inductive
Research	Form hypotheses	Test hypotheses	Establish generalized theories
Investigation	Develop scenarios	Fact-check scenarios	Make investigative decisions
Testimony	State claims[3]	Fact-check claims	Evaluate traces apropos of the claims

Table 1: Application of abductive, deductive, and inductive reasoning to research, investigation and testimony.

The ability to separate these multiple modalities, sometimes carried out by the same person, and sometimes by different people, while integrating their collective results in a manner that can be used in a legal context is the core objective of forensic science.

In forensic science research, this scientific reasoning process is used to formulate hypotheses to explain observations, test those hypotheses against predicted consequences, and interpret experimental results in relation to a new or existing generalized theory. During an investigation, practitioners develop scenarios that could explain available evidence, search for contradictory and predicted facts, and interpret available information to reach an investigative decision. When preparing testimony, practitioners use this scientific reasoning process to take specific claims (plaintiff, defense, other), fact-check the claims against traces (look for predicted traces and contradictory traces), and evaluate the observed traces apropos of each claim. In such situations, forensic scientists are given a specific claim (e.g., by an attorney or judge), but this does not eliminate the need to exercise abductive reasoning to formulate alternative explanations. Looking for evidence that disproves a given claim (falsification) improves all phases of inquiry and thus is the embodiment of the methodology, as advocated by Peirce and other pragmatist philosophers of science, to be the foundation of the physical and life sciences (Popper, 1963).

It is also important to realize that scientific reasoning leads to probabilistic statements, not certainty in conclusions. The outcome of scientific reasoning does not represent objective reality or "ground truth," but rather provides a prediction about what might be true given currently available knowledge and observable traces. Many scientific processes can be limited by available evidence and current knowledge, even sometimes skewed by cognitive bias, and influenced by external pressures such as deadlines and fatigue. At the same time, the judicial system requires a decision, made by decision-makers other than forensic scientists, and operates with the understanding that truth may not be fully known within the limited timeframe of an investigation and the associated legal proceedings.

[3] A *claim* is an assertion that something is true (Merriam-Webster). Some forensic scientists prefer to use the synonymous term *proposition*, which is an assertion that expresses an opinion that can be true or false (Merriam-Webster). In a legal context, claims can be raised by a party to a legal dispute; claims may also be raised and evaluated by investigators and forensic scientists.

5.1. Core Forensic Processes

After extensive research, surveys, and discussions, the TG identified five core processes to address forensic questions: authentication, identification, classification, reconstruction, and evaluation.

Understanding of core forensic processes can be confounded by inconsistencies in terminology between disciplines. For instance, the term *identification* is used in many forensic disciplines to describe a core process as discussed further in this section. However, in the context of digital evidence, *identification* is sometimes defined differently as "a process involving the search for, recognition and documentation of potential digital evidence" (ASTM, 2015). Furthermore, in the context of facial identification, *identification* is used to describe the results of searching a database for potential matches to a specific unknown entity (ASTM, 2015). Some disciplines even eschew the term *identification* to avoid the confusion cause by differing definitions.

A primary purpose of the TG was to broaden the discussion of forensic questions beyond discipline specific terminology. To this end, the labels used in this document (authentication, identification, classification, reconstruction, and evaluation) refer to fundamental concepts and processes that go beyond disciplines specificities. These concepts are applied in specific ways in numerous forensic disciplines and contexts, and sometimes are even described using other terminology. The underlying concepts and processes are the focus of this document to clarify their precise meaning as they apply to digital/multimedia traces, and to highlight commonalities across other forensic disciplines. To assist the reader in understanding and applying these core processes, samples of forensic questions are categorized in Appendix 1.

To facilitate discussions across forensic disciplines independent of specific terminology, the TG developed generalized definitions for core forensic processes, and applied these definitions in the context of digital/multimedia evidence. These definitions form a coherent set of intertwined definitions that harmonize concepts and practices within digital/multimedia science, and may potentially be useful across most forensic disciplines, articulating their scientific basis and promoting forensic science as one science.

To emphasize the integral and crucial role of evaluation in the decision within other core forensic processes, the term *sufficient confidence* is repeated in most definitions. The term sufficient confidence is intentionally general to cover different kinds of evaluation in different contexts, including strength of evidence, and potentially using a coverage interval.[4] In a given context, the decision-maker will set a decision threshold for the minimum acceptable level of confidence that must be reached. For instance, in courtroom contexts, it is the role of the decision-maker (e.g., judge or jury) to set a threshold and reach a decision. In this context, it is the role of forensic scientists to report their trace evaluation results, which is sometimes termed the strength of evidence, and to help the decision-maker reach a decision. Outside of the courtroom, there are other contexts in which forensic scientists themselves must reach a decision on the basis of some threshold.

[4] NIST policy is to use ISO Guide 98, "Guide to the Expression of Uncertainty in Measurement (GUM)" which uses coverage intervals, not confidence intervals (Wayman, 2013).

Authentication: ***Decision process attempting to establish sufficient confidence in the truth of some claim*** (Jaquet-Chiffelle, 2009b adapted from National Research Council, 2003).

Any authentication process (forensic or not) can be subdivided into two consecutive sub-processes: a claim evaluation sub-process, followed by the actual decision sub-process based on a threshold. During the claim evaluation sub-process, the level of confidence of the claim is established. Then this value is passed to the decision sub-process. If the established level of confidence is higher than the threshold, the result of the decision is positive and the authentication successful. It is important to emphasize that an authentication process does not necessarily result in certainty.

Authentication
In a forensic context, the claim to authenticate can include the integrity and provenance of a trace, as well as contextual descriptions and temporal restrictions. In the context of access control using biometric features, authentication establishes, to some level of confidence, whether or not the person is who he claims to be.

Identification: ***Decision process attempting to establish sufficient confidence that some identity-related information describes a specific entity in a given context, at a certain time*** (Casey & Jaquet-Chiffelle, 2017; Jaquet-Chiffelle, 2009b).

Identification can be applied not only to human beings, but also to animate or inanimate entities, physical or virtual. In general, several entities might be described by the same information. Identification attempts to ascribe a specific entity to the group of entities described by this same information, in this same context, at that time.[5] Any identification process comprises two consecutive sub-processes: the selection sub-process, followed by the authentication sub-process. During the selection sub-process, at least one quadruplet (entity, identity-related information, context, time) is selected for potential successful identification. For example, when the identification is a simple verification of identity (e.g. when a user tries to access his email account, or when a traveler presents himself at a border), only one quadruplet is typically selected. As another example, when searching a database for identity-related information that potentially matches a specific (unknown) entity, quadruplets are generated for each retrieved record in the database. During the second phase, for each selected quadruplet, a *corresponding claim* is fed into the authentication sub-process: *"This entity is described by this identity-related information in this context at that time."* The outcome of the identification process depends on the result of the authentication of these corresponding claims.

Classification: ***Development of taxonomies of traces and the decision process attempting to ascribe a trace with sufficient confidence to its class on the basis of characteristics that are common among traces of the same class, distinguishing them from traces of other classes***.

Class characteristics may depend on both the traces and the events (e.g. actual activities) that led to the traces. Forensic classification, like classification in other scientific disciplines, has

[5] When the group is reduced to exactly one entity, some forensic scientists call this result of the identification process *individualization* (Kirk, 1963; Inman and Rudin, 2002). In practice, individualization of an entity is only feasible within a specific context and time, not universally (Champod and Evett, 2001; Cole, 2009). To reduce confusion, forensic scientists are clarifying the distinction between individuality and identification, and are eschewing the use of the term *individualization* (Robertson et al., 2016; Champod, 2013).

two facets. One facet is taxonomy, the scientific process that creates and defines classes. For a given taxonomy, each class is defined by a set of characteristics that is shared by traces in this class, but differs for other traces. The other facet is ascription, the process that recognizes, with sufficient confidence, an element as belonging to its specific class. This second facet can be considered as *trace identification* within the context of a taxonomy.

Reconstruction: ***Organize observed traces to disclose the most likely operational conditions or capabilities (functional analysis), patterns in time (temporal analysis), and linkages between entities – people, places, objects – (relational analysis)***.

For transparency reasons, the level of confidence reached for a reconstruction should be expressed clearly. What is most likely can depend on concealment behavior and the skill level of an offender (Casey, 2013).

Evaluation: ***Produce a value that can be fed into a decision process.***

Evaluation appears intensively in forensic science, both as a top process (e.g. in courtroom contexts) and as a sometimes implicit deep sub-process within other core processes. The concept of evaluation is broad and sometimes controversial.

In order to avoid confusion, it is useful to make a clear distinction between two categories of evaluations: *concrete* evaluation and *abstract* evaluation. Concrete evaluation takes place in the "real" world, in our concrete universe. In a legal context, a judge or a jury is responsible both for concrete evaluations that feed a court decision, and for the subsequent court decision itself. Abstract evaluation occurs in an abstract and hypothetical universe where some (extra) assumption (typically a claim) is considered *by definition* to be true. Therefore, this assumption is never questioned nor evaluated within this abstract universe; actually NO decision about it would make sense inside this hypothetical universe. At the very most, if the assumption leads to a contradiction, the existence of the abstract universe is denied and the assumption disproved.[6]

Evaluation □ Decision

The value produced by evaluation can be a measure of a continuous nature, such as a real number between 0 and 1 (probability), or a real number between -1 and 1 (measure of distrust and trust). Alternatively, this value can be a mark of a discrete nature, such as {A+, A, A-, B+, B, B-, C, D, F}, {*, **, ***, ****}, {excellent, good, satisfying, sufficient, insufficient}, or a verbal scale.

This value can be used later □ sometimes in combination with other values or information □ to reach a decision. The decision chooses an outcome within a finite number of possibilities, such as {yes, undecided, no}, {guilty, not guilty}, and {low confidence, medium confidence, high confidence}.

It is essential to emphasize that any decision process (e.g., identification, authentication) being fed by evaluation is a subsequent and separate process that can even be performed by a different entity than the one performing the evaluation. In courtroom contexts, forensic scientists evaluate traces, and help the judge or jury make decisions.

[6] Notably, there is a risk of hidden assumptions being included in such abstract universes which can bias the evaluation process.

In courtroom contexts, when forensic scientists perform a *trace evaluation*, at least two (competing) claims need to be considered in order to prevent some forms of bias: typically a plaintiff's claim and its denial by a defendant. The truth of these claims should never be evaluated by the forensic scientists. Each competing claim becomes the *true assumption* defining one corresponding abstract universe; then an abstract evaluation of the trace is performed in each of those hypothetical universes. When forensic scientists perform (abstract) trace evaluation, they provide a value, sometimes referred to as the *strength of evidence*. Results of these abstract evaluations are sometimes summarized as a likelihood ratio (LR), i.e. the ratio between the probability to observe the trace in the first universe (e.g. if the plaintiff's claim is true) and the probability to observe it in the competing universe (e.g. if the plaintiff's claim is not true) (Aitken & Taroni, 2004).

At a second stage, a judge or jury will have to assess whether the claim is true or not in the real world. Formally, in order to take a judicial decision, a judge or jury will try to authenticate some claim(s), typically a claim based on the plaintiff's claim and/or another one based on the opposing claim. The value produced by *trace evaluation* can establish the strength of evidence apropos of a claim, or disprove the claim. In some cases, (abstract) evaluation of traces can result in a high strength of evidence apropos of a claim, but consideration of other information can result in zero confidence in the corresponding claim. For example, there could appear to be a high strength of evidence apropos of the claim that a particular person was involved in a crime, but the person has an airtight alibi or was deceased, resulting in zero confidence in the claim that this person was actually involved in this crime. During the authentication process, the judge or jury concretely evaluates the claims, combining the strength of evidence or likelihood ratio with all other relevant information for the case (e.g., alibi), and forms an interpretation of this information in order to decide whether or not there is sufficient confidence in the truth of a claim to condemn the suspect.

Strength of Evidence versus Strength of Hypothesis

In courtroom contexts, it is inappropriate for forensic scientists to deliver conclusions about the strength of a hypothesis (i.e., the probability that a particular hypothesis is true). The strength of hypothesis approach encroaches upon (concrete) claim evaluation, which must take into account the full information in a case. In courtroom contexts, claim evaluation is the responsibility of decision-makers such as a judge or jury (Champod & Taroni, 2017); for example, deciding whether the forensic findings regarding identification are sufficient to implicate the defendant (also taking into consideration other facts in the case). In courtroom contexts, to avoid encroaching upon the role of decision-maker, forensic scientists must exercise caution when expressing the probative value of forensic findings, concentrating on the well-established knowledge of traces in their domain of expertise rather than on the claim under consideration. In facial identification, a strength of hypothesis approach, which is inappropriate, would state the conclusion "It is more likely that the person depicted in image X is the same as the person depicted in image Y given the observed traces." The correct approach, a strength of evidence approach, would state the conclusion "The observed traces are more likely under the claim that the person depicted in image X is the same as the person depicted in image Y." In short, a strength of hypothesis approach is directed at supporting the claim whereas a strength of evidence approach is directed at evaluating traces.

Also keep in mind that the definition of forensic science in Section 2 of this document uses legal context in the broadest terms. Forensic scientists should not be reduced to experts only in courtroom contexts. There are numerous situations where forensic scientists need to make decisions (outside of their evaluation role in courtroom contexts) and perform the concrete evaluations that precede these decisions. This is particularly true in the investigation phase or when the issues at stake do not involve a civil or criminal justice system. For example, forensic scientists may have to identity victims of a tsunami; the decision of who is who in such a situation is not taken by a judge.

The core forensic processes interact with each other in various ways.

- Authentication is used within the identification, classification, reconstruction, and evaluation processes to support the establishment of sufficient confidence in the truth of sub-claims within each of these core forensic processes.
- Identification is used within the authentication, and classification, and evaluation processes. Some forensic scientists use the term "source identification" to refer to the highest level of confidence when the authentication process is applied to the forensic question of whether or not an item came from a specified source.
- The ascription facet of trace classification can be considered as trace identification within the context of a taxonomy.
- Reconstruction can be a sub-process within authentication, identification, classification, and evaluation. Conversely, to ensure completeness and correctness, reconstruction typically relies on results from the other core forensic processes.
- Evaluation precedes every decision in the forensic lifecycle, including those in the core forensic processes defined in this document.

To clarify how identification-related claims are authenticated in different contexts, several comparative examples are shown in Table 2.

Context	**Claims**	**Evaluation (forensic scientist)**	**Decision (judge / jury)**
Facial identification	Same/Not Same source (face)	High strength of evidence apropos of the claim of Same Source over the other claim, and no contradictory traces	Same source (face)
Image/video analysis	Same/Not Same source (camera)	Low strength of evidence apropos of the claim of Same Source over the other. Or traces were found that disprove the claim of Same Source (falsification).	Not same source (camera)

Digital evidence	Same/Not Same source (computer)	High strength of evidence apropos of the claim of Same Source over the other claim, and no contradictory traces	Same source (computer)
Fingerprint	Same/Not Same source (finger)	Low strength of evidence apropos of the claim of Same Source over the other claim. Or traces were found that disprove the claim of Same Source (falsification).	Not same source (finger)
Biometric access control	Same/Not Same source (face, voice, fingerprint, iris)	High strength of evidence apropos of the claim	Permit access

Table 2: Examples of authentication of identification-related claims in different contexts.

5.2. Forensic Activities

Forensic science applies the following activities to study traces:

- Survey: search, find, detect, recognize traces.
- Preservation: protect traces from alteration (e.g., isolating them from surrounding environment), collect traces in a manner that changes as little as possible, and evidence management activities such as storing evidential items.
- Examination: observe traces and their characteristics, recover information or content from data sources, and make the results available for analysis.[7]
- Documentation: record traces, along with their associated context, characteristics, forensic activities, and provenance information.
- Analysis: process traces to obtain more information about their characteristics, and make the results available for integration, classification, reconstruction, and evaluation or interpretation. Analysis utilizes the results of the examination forensic activity, and places them into a technical context.[8]
- Integration: combine results of multiple analysis processes to obtain a more comprehensive understanding of traces, typically to support the forensic reconstruction process, as well as the interpretation.
- Interpretation: explain the meaning of forensic findings to help reach decisions in forensic investigations and to help establish general theories in forensic research. In courtroom contexts, forensic scientists perform evaluations to help decision-makers understand and interpret the implications of the evaluation in the broader context of the case.

[7] Facial identification refers to this activity as analysis.
[8] Facial identification refers to this activity as examination.

These activities, and the information they produce, feed the core forensic processes of authentication, identification, classification, reconstruction, and evaluation. Accreditation and best practices typically increase the level of confidence in these activities and in the resulting information.

6. Operational Techniques

After extensive research, surveys, and discussions, the TG recognized several additional operational techniques that do not directly address specific forensic questions, but provide the necessary information and support for the forensic activities and support for core forensic processes. For example, these operational techniques for digital/multimedia evidence include:

- Preservation techniques: capture evidence in a manner that establishes its original context and changes as little as possible. Provide necessary technical tools for the *preservation* forensic activity. This technical step is of utmost importance to maintain trace integrity which is essential to reach trace authenticity.
- Recovery techniques: salvage information or content from data sources that otherwise cannot be accessed.
- Enhancement and restoration techniques: bring out details in images, video, or audio that otherwise cannot be discerned clearly, without causing adverse or discriminatory impact. Provide necessary technical tools for revealing traces that are difficult to see and making them available for subsequent forensic activities and core forensic processes.[9]

Validation typically increases the level of confidence in these operational techniques.

7. General Lessons

When dealing with non-biometric information, it is important to differentiate between a physical person (human being) and the (virtual or not) entity under scrutiny (e.g. an email or user account, the user of a credit card, etc.). The model of "virtual persons" developed within the Future of Identity in the Information Society project allows faithful capture and representation of these distinctions (Jaquet-Chiffelle, 2008, 2009a, 2009b).

When forming a forensic question, it is important to state it in a way that can be verified or falsified, i.e. in a claim that can be authenticated. For example, instead of, "Is this recording authentic or unedited?", corresponding competing claims that can be evaluated are "This recording is authentic," and "This recording has been altered or edited."

[9] Amplification could be considered a form of enhancement, which applies to audio, video, and DNA.

8. Conclusions and Recommendations

The deliberations of the OSAC Task Group on Digital/Multimedia Science have resulted in the development of a framework and definitions that can be used for harmonizing concepts and practices within digital/multimedia science, and may potentially be useful across most forensic disciplines. In this document, forensic science is treated in the broad sense to include the typical criminal, civil, and regulatory functions of the legal system, as well as its extensions such as human rights, employment, natural disasters, security matters. Within this context, the TG considered how digital/multimedia evidence meshes with forensic science as a whole.

This work describes how forensic science iteratively utilizes abductive, deductive, and inductive reasoning. The document articulates the five core forensic processes identified and defined by the TG: authentication, identification, classification, reconstruction, and evaluation. It further identifies and defines seven forensic activities that support the study of traces: survey, preservation, examination, documentation, analysis, integration, and interpretation. Three additional operational techniques are described that support forensic activities: preservation, recovery, and enhancement and restoration.

The TG realized that digital/multimedia evidence, and other forensic disciplines, would be in a much stronger position to demonstrate their scientific basis if they were considered as belonging to a harmonized forensic science rather than as mere disciplines at the intersection of forensic specialties and other sciences. The new paradigm created by the digital realm brings a unique opportunity to revisit fundamental definitions in forensic science and to strengthen the identity of forensic science as one science, unified by common principles and processes that can address questions for legal contexts including, but not restricted to, problems that do not have prior probabilities or well-established knowledge.

The following recommendations flow from this work to advance digital/multimedia evidence, and forensic science as a whole.

- Use the framework and definitions in this work to facilitate discussion between forensic disciplines in order to establish commonalities and differences across forensic science.
- Strengthen scientific foundations of digital/multimedia evidence by developing systematic and coherent methods for studying the principles of digital/multimedia evidence to assess the causes and meaning of traces in the context of forensic questions, as well as any associated probabilities.
- Differentiate between core forensic processes, forensic activities, and operational techniques.
- Assess ways to mitigate cognitive bias in cases that require an understanding of the context of traces in order to analyze digital/multimedia evidence, e.g., reconstruction.
- Distinguish between a physical person and the entity under scrutiny, (e.g. an email or user account, the user of a credit card, etc.).

- Contribute to understanding the core forensic process of identification in the context of digital/multimedia evidence, study new ways to attribute online activities to (physical) individuals using digital traces, and validate the reliability of these methods.

- Establish effective ways to evaluate and express probative value of digital/multimedia traces for source level and activity level conclusions. This includes studying how quantitative evaluation of digital/multimedia evidence can be constructed for different forensic questions, including reconstruction, as well as studying how such evaluative results can be communicated to decision-makers.

This document is part of the ongoing cultivation of the structure, processes, and approaches of digital/multimedia evidence in particular, and forensic science in general. Forensic science is combining education, research, and casework to advance as a scientific field in its own right (Margot, 2011b). As forensic science continues to mature, these notions will continue to evolve. That is, after all, the intrinsic nature of science.

Acknowledgements
The authors are grateful to the OSAC for motivating and reviewing this effort, particularly Richard W. Vorder Bruegge for his recognition of importance of addressing the central questions in our field, his stalwart support of the Task Group, and his insights throughout the process of compiling this document. We thank the dedicated members of the OSAC Task Group on Digital/Multimedia Science (Mark Pollitt, Eoghan Casey, Pavel Gladyshev, David-Olivier Jaquet-Chiffelle, Martin Olivier, Michael Piper, Lam Nguyen, Henry Reeve, Marcus Rogers).

James Darnell, Douglas Lacey, Lora Sims, James Wayman, Julie Carnes, and other members of the Digital/Multimedia SAC and subcommittees for their insights that helped guide and refine this work.

The authors want to thank their colleagues Alex Biedermann, Christophe Champod, Simone Gittelson, and Olivier Ribaux who reviewed drafts of this document and contributed to its technical content.

The authors would also like to express their thanks to JoAnn Buscaglia, Gregory Davis, Lucy Davis, Laurel Farrell, Melissa Gische, George Herrin Jr., Karen Kafadar, Sarah Kerrigan, Jeff Salyards, Bill Thompson, and other members of the Forensic Science Standards Board for their refining recommendations.

Dedication
This document is dedicated to the memory of Carrie Morgan Whitcomb, who was both a source of ignition and accelerant in the development of digital evidence as a forensic science. As a forensic scientist, leader, and mentor, her contributions to the field will be enduring.

References

Aitken CGG, Taroni F (2004) *Statistics and the evaluation of evidence for forensic scientists*. John Wiley & Sons, Chichester.

ASTM (2015) *Standard Terminology for Digital and Multimedia Evidence Examination*. ASTM E2916 − 13

Biedermann A (2015) The Role of the Subjectivist Position in the Probabilization of Forensic Science. *Journal of Forensic Science and Medicine.* Volume 1, Issue 2, Pages 140-148. Available at https://doi.org/10.4103/2349-5014.169569

Biedermann A, Vuille J (2016) Digital evidence, 'absence' of data and ambiguous patterns of reasoning. Presented at the DFRWS EU 2016 conference, published in *Digital Investigation,* Volume 16, Supplement, Pages S86-S95. Available at http://www.dfrws.org/2016eu/program.shtml

Casey E (2011) *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. (3rd edition). Waltham, MA: Academic Press.

Casey E (2013) *Reinforcing the Scientific Method in Digital Investigations using a Case-Based Reasoning (CBR) System*. PhD Dissertation, University College Dublin.

Casey E, Jaquet-Chiffelle D-O (2017) Do Identities Matter? *Policing: a Journal of Policy and Practice, Special Issue*. Oxford: Oxford University Press. Available at https://doi.org/10.1093/police/pax034

Champod C, Taroni F, *A Probabilistic Approach to the Evaluation of Fibre Evidence*. In: J. Robertson, C. Roux, Forensic Examination of Fibres. 3rd edition. CRC Press, Boca Raton (2017) in press

Chisum J, Turvey B (2011) *Crime Reconstruction*. (2nd edition). Waltham, MA: Academic Press.

Crispino F (2008) Nature and Place of Crime Scene Management in Forensic Sciences. *Science & Justice.* Volume 1, pp. 24-28. Available at https://doi.org/10.1016/j.scijus.2007.09.009

DeForest P, Gaensslen R, Lee H (1983) *Forensic Science: An Introduction to Criminalistics*. New York: McGraw Hill.

Dror I (2011). *The paradox of human expertise: why experts get it wrong*. In N. Kapur (Ed.), The paradoxical brain (pp. 177-188). Cambridge: Cambridge University Press.

Dror I (2015) Cognitive and Human Factors. Chapter 4 in *Annual Report of the Government Chief Scientific Adviser 2015: Forensic Science and Beyond: Authenticity, Provenance and*

Assurance, Evidence and Case Studies. London: Government Office for Science. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/506462/gs-15-37b-forensic-science-beyond-evidence.pdf

Douven I (1999) Inference to the Best Explanation Made Coherent, Philosophy of Science, Supplement. Proceedings of the 1998 Biennial Meetings of the Philosophy of Science Association. Part I: Contributed Papers (Sep., 1999), Volume 66, Pages S424-S435.

Eco U, Sebeok TA (1983) *The Sign of Three: Dupin, Holmes, Peirce (Advances in Semiotics)*. Bloomington, IN: Indiana University Press

ENFSI (2015) *ENFSI guideline for evaluative reporting in forensic science*. (Approved version 3.0). Available at http://enfsi.eu/sites/default/files/documents/external_publications/m1_guideline.pdf

Fenton N, Neil M, Berger D (2016) Bayes and the Law. *Annual Review of Statistics and Its Application*. Volume 3, Pages 51-77. Available at http://dx.doi.org/10.1146/annurev-statistics-041715-033428

Gisolf F, Malgoezar A, Baar T, Geradts Z (2013) Improving source camera identification using a simplified total variation based noise removal algorithm. *Digital Investigation*, Volume 10, Issue 3, Pages 207–214. Available at https://doi.org/10.1016/j.diin.2013.08.002

Gross H (1924) *Criminal Investigation*. London: Sweet & Maxwell.

van Houten W, Alberink I, Geradts Z (2011) Implementation of the likelihood ratio framework for camera identification based on sensor noise patterns. *Law, Probability and Risk*, Volume 10, Issue 2, Pages 149-159. Available at https://doi.org/10.1093/lpr/mgr006

International Association of Computer Investigative Specialists (1990) *IACIS History*. Available online at http://www.iacis.com/Pages/History.aspx

Inman K, Rudin N (2001). *Principles and Practices of Criminalistics: The Profession of Forensic Science*. Boca Raton, FL: CRC Press.

Jackson G, Jones S, Booth G, Champod C, I.W. Evett (2006) The nature of forensic science opinion—a possible framework to guide thinking and practice in investigation and in court proceedings. *Science & Justice*, Volume 46, Issue 1, Pages 33-44. Available at http://dx.doi.org/10.1016/S1355-0306(06)71565-9

Jaquet-Chiffelle D-O (2008) The Model : A Formal Description, Section 7.2. In D-O Jaquet-Chiffelle, B Anrig, E Benoist, and R Haenni, eds., *Virtual Persons and Identities*, FIDIS deliverable 2.13. Available at http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp2-del2.13_Virtual_Persons_v1.0.pdf

Jaquet-Chiffelle D-O (2009a) Identity Core Components, Section 7.2. In D-O Jaquet-Chiffelle, H Buitelaar, and B Anrig, eds., *Modelling New Forms of Identities: Applicability of the Model Based on Virtual Persons,* FIDIS deliverable 17.1. Available at http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp17-del17.1.Modelling_New_Forms_of_Identities.pdf

Jaquet-Chiffelle D-O (2009b) Identification, Section 4.2. In D-O Jaquet-Chiffelle and H Buitelaar, eds., *Trust and Identification in the Light of Virtual Persons,* FIDIS deliverable 17.4. Available at http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables/fidis-wp17-del17.4_Trust_and_Identification_in_the_Light_of_Virtual_Persons.pdf

Jaquet-Chiffelle D-O (2013) "Traces : New Definition." Course Introduction à la criminalistique numérique, University of Lausanne, School of Criminal Justice. Available at https://serval.unil.ch/resource/serval:BIB_DFE9D125DECA.P001/REF

Jaquet-Chiffelle D-O (2014) Digital forensics : Betrachtungen zu einer neuen Disziplin. *Kriminalistik*, Volume 68, Issue 3, Pages 188-190.

Kennedy D (2003) Forensic Science: Oxymoron? Science. Volume 302. Page 1625

Kuhn T (1996) *The Structure of Scientific Revolutions*. Chicago, IL: University of Chicago Press.

Lipton P (2004) *Inference to the Best Explanation*. (2nd edition). London: Routledge

Margot P (2003) Course in Forensic Science, University of Lausanne, School of Criminal Justice.

Margot P (2011a) Forensic science on trial - What is the law of the land? *Australian Journal of Forensic Sciences*. Volume 43, Issue 2-3, Pages 89-103.

Margot P (2011b) Commentary on the need for a research culture in the forensic sciences. *58 UCLA LAW REVIEW*, Pages 795-801.

Minnaard W (2014) Out of sight, but not out of mind: Traces of nearby devices' wireless transmissions in volatile memory. *Digital Investigation*, Volume 11, Supplement 1, Pages S104–S111. Available at http://www.dfrws.org/2014eu/program.shtml

National Research Council (2003) *Who Goes There?: Authentication Through the Lens of Privacy.* Washington, DC: The National Academies Press. Available at https://doi.org/10.17226/10656

National Research Council (2009) *Strengthening Forensic Science in the United States: A Path Forward.* Washington, DC: The National Academies Press. Available at https://doi.org/10.17226/12589

Pollitt M (1995) “Computer Forensics: An Approach to Evidence in Cyberspace.” Proceedings of the 18th National Information Systems Security Conference. Pages 487-491.

Pollitt M (2008) Applying Traditional Forensic Taxonomy to Digital Forensics. In I Ray and S Shenoi, eds., *Advances in Digital Forensics IV*, Pages 17–26. Heidelberg: Springer.

Pollitt M (2013) History, Historiography, and the Hermeneutics of the Hard Drive. In G Peterson and S Shenoi, eds., *Advances in Digital Forensics IX,* Pages 3-17. Heidelberg: Springer.

Popper K (1963) *Conjectures and Refutations*. London: Routledge and Keagan Paul.

Reust J, Sommers R (2008) “Identification and Reconstruction of Deleted, Fragmented DNA Digital Files.” presented at the American Academy of Forensic Sciences 2008 Annual Meeting.

Ribaux O (2014) *Police scientifique: Le renseignement par la trace*. Lausanne: Presses polytechniques et universitaires romandes.

Richter MM, Aamodt A (2005) Case-based reasoning foundations. *Knowledge Engineering Review*, Volume 20, Issue 03, Pages 203-207.

Risinger DM, Saks MJ, Thompson WC, Rosenthal R. (2002). *The Daubert / Kumho implications of observer effects in forensic science: hidden problems of expectation and suggestion*. California, Law Review, 90: 1–55.

Rudin K, Inman N (2002) The origin of evidence. *Forensic Science International,* Volume 126, Pages 11-16.

Saferstein R (2000) *Criminalistics: An Introduction to Forensic Science* (7th edition). Upper Saddle River, NJ: Prentice Hall.

Scientific Working Group on Digital Evidence (2017) *Establishing Confidence in Digital Forensic Results by Error Mitigation Analysis*. SWGDE, Version: 1.7 Available at https://www.swgde.org/documents/.

Sunde N (2017) *Non-technical Sources of Errors When Handling Digital Evidence within a Criminal Investigation*. Master’s thesis. Norwegian University of Science and Technology.

Turvey B (2011) *Criminal Profiling: An Introduction to Behavioral Evidence Analysis* (4th edition). Cambridge, MA: Academic Press.

Tversky A, Kahneman D (1974) Judgment under Uncertainty: Heuristics and Biases. *Science,* New Series, Volume 185, Number 4157, Pages 1124-1131.

Unites States v. Marvin Hersh (2002), United States 11th Circuit Court. Available at http://caselaw.findlaw.com/us-11th-circuit/1260649.html

Wayman J, Possolo A, Mansfield AJ (2013) Modern statistical and philosophical framework for uncertainty assessment in biometric performance testing. IET Biometrics, Volume 2, Number 3, Pages 85-96.

White D, Phillips PJ, Hahn CA, Hill M, O'Toole AJ (2015) Perceptual Expertise in Forensic Facial Image, *Proceedings. Biological sciences / The Royal Society*, Volume 282(1814). Available at https://doi: 10.1098/rspb.2015.1292.

Wisse W, Veenman C (2015) Scripting DNA: Identifying the JavaScript programmer. *Digital Investigation*, Volume 15, Pages 61-71.

Appendix 1: Sample Forensic Questions

The following are examples of forensic questions in the context of digital/multimedia evidence. These forensic questions are stated as claims that would be evaluated against competing claims. The aim of stating forensic questions in terms of opposing claims is to mitigate the risk of bias.

Authentication

- These two files are the same at a binary level.
- These two files are the same at the semantic level (fuzzy hashes).
- These two files are the same at the content level.
- This recording is authentic and unaltered.
- The file was created at the time specified by the file system.
- This photograph is authentic or unaltered.
- The clock was correct on the computer.
- The time on the computer was changed.
- The device was set to automatically change the clock.
- This image was taken in Location X.
- The wireless is not authentic or was spoofed.
- This device connected to file share X.
- The computer is infected/compromised with malware.
- An unauthorized Entity gained access to the computer.
- This communication is the original authoritative source(s).

Identification

- Person X is the person in the recording.
- The person in the images are the same person.
- Entity X caused the event.
- This computer was last accessed by Entity X.

- This image was last accessed by Entity X.
- Entity X accessed this server from Location Y.
- Device X (specific) was used to capture this media.

Classification

- The photograph is a JPEG file.
- The device is a Samsung SMG900P Galaxy S5.
- The data is a credit card number.
- The accent of the voice in the recording is Irish.
- The malware is crypto-ransomware.

Reconstruction

- Reconstruct any traces of data deletion, erasure, or wiping, including the time of deletion.
- Reconstruct any traces of data deletion, erasure, or wiping, including motivation of deletion.
- Reconstruct any communication between Entity X and Entity Y.
- Reconstruct what programs were executed with this device.
- Reconstruct any connections between this device and wireless access points.
- Reconstruct any files copied from the device and to another device.
- Reconstruct a timeline of user activity on the computer.
- Reconstruct any connections between this device and a mobile device.
- Reconstruct all Entities that accessed this image, including when.
- Reconstruct any connections between this device and physical storage.
- Reconstruct any connections between this device and cloud based storage.
- Reconstruct all user access to this server, including their location (console) or computer address (IP address, Server Message Block (SMB) name).

- Reconstruct how many Entities used the device.
- Reconstruct any access control or restrictions on the file share, including Access Control Lists (ACLs) on the share, IP filters on the server, and firewall or router rules on the network.
- Reconstruct any traces of data being stolen from this computer.
- Reconstruct any traces of a vulnerability being exploited in this web application.

Evaluation

- The observed traces are more likely given one claim, and less likely given the other claims.
- The specific web searching activities in question were performed by user actions on the computer with User Account X.
  Note: this is an abstract claim that would be considered by a forensic scientist when evaluating the strength of evidence apropos this claim. This would be accompanied by an evaluation of the opposing (abstract) claim that the web searching activities were not performed by user actions on the computer with User Account X.
- Concrete claim: The specific web searching activities in question were performed by the suspect.
  Note: this is a concrete claim that would be considered by decision-makers, considering all other relevant information for the case, including the strength of evidence from the forensic scientist's evaluation of the abstract claims (above).

Appendix 2: Sample Operational Techniques

The following are examples of operational techniques for digital/multimedia evidence that provide necessary information for the forensic analysis or to address forensic questions:

Preservation Techniques

- Data on this device can be acquired or copied in a manner that is complete and accurate, without making substantive changes.

Recovery Techniques

- This device contains a deleted spreadsheet containing financial information.
- This device contains metadata about files that have been deleted.
- This device contains content from files that have been deleted.
- This device contains metadata about sensitive files that were on the device.
- This device contains content from files that were on the device.
- This device contains information that will unlock the mobile devices.
- This device contains information that will unlock online accounts the user accessed with this device.
- This encrypted device or file can be decrypted.
- This device contains information that will decrypt data.
- This damaged or legacy device or file contains information that can be recovered.
- This damaged or legacy device or file contains information that can be recovered with reasonable effort or expense.
- This damaged or legacy device or file contains information that can be recovered with significant effort or expense.

Enhancement Techniques

- Content in this digital photograph can be made clearer.
- Voices in this audio recording can be made more clear or audible.