This chapter describes common scenarios in the work of forensic document examiners (FDEs), the objects they examine and the goals of the expertise. To calibrate their intended research projects it is important that computer scientists know and understand what the issues are that FDEs have to solve.

Ecosystem: The FD universe

A succinct definition of forensic science is “science used for the purpose of the law.”¹ It implies that there are a multitude of nonforensic sciences involved in forensics, as well as there being scientific constructs proper to the forensic field. Forensic documents (FD), also known as questioned documents, is in turn the science of document examination as applied to legal cases. Etymologically “forensic” refers to the Roman-time fora where trials were conducted, and “forensics” being—depending on the usage—the act of presenting the evidence, shorthand for “forensic science,” or—by suppressing the term “science”—avoidance of debates on the scientific quality of the field.²

One among many forensic areas, FD is divided into a number of specialties, and linked to numerous fields outside forensics, not unlike computer science.³ Some of its branches deal with the material aspects of documents, the hardware, so to speak (instruments, ink, paper), and others with patterns (writing), behavioral traces of human activity characterized by great variability.⁴ FD is closely related to biometrics and security documents, despite theoretical and institutional compartmentalization.⁵ Among the forensic fields FD is the smallest entity,⁶ which means on one hand that it has a sufficient individuality to maintain its independence, and on the other hand that it is of marginal importance, a trend accentuated by the advent of forensic DNA profiling in the 1980s and visible in the proportion of published FD articles.⁷ As one FDE put it in his memoirs: “I belong to one of the smallest and least understood professions in the world.”⁸

Inside FD proper, there is slightly more research activity around the material aspects of FD, than for patterns. Overall, handwriting and paints analysis are by far the most important areas, yet the diversity of study topics is clearly visible. We see a predominance of hardware-based analysis for the material aspects and software-based for patterns; digital media analysis is a rising area, with a foothold in both FD and digital media forensics; computing resources are a fairly small portion of the issues debated, of steady interest in time; statistics has a rising trend; demographics is of little concern. The entry and exit of researchers and projects affect the fluctuation in time of various fields: handwriting software and statistics can be clearly traced to research groups at CEDAR (Buffalo, NY), George Mason University (Fairfax, VA), and École des sciences criminelles [School of forensic science] (Lausanne, Switzerland). Although the publications on which this analysis is based are just a fraction of the FD computing research—the majority of work being published in computing and mathematics publications—they are a good indicator of how many software prototypes evolved toward deployment in day-to-day forensic work.

Conspicuously absent from the conferences of the American Academy of Forensic Sciences (AAFS), a major venue for forensics, are other research groups active in computing, biomechanics, and neurocognitive aspects of handwriting (e.g., for identification the University of Groningen [Netherlands]; for biomechanical signal modeling and analysis the École Polytechnique [Montreal, Canada], the University of Arizona [Phoenix, AZ], and the Radboud University [Nijmegen, Netherlands]). For some of them, the International Graphonomics Society (IGS) conferences are the privileged meeting place, where FD and computing converge. Signature computing gyrates around the venues of the biometrics market, where their more substantial applications lie. Finally there is yet another area with fleeting presence at AAFS: security documents, which—heavily commercialized and relying on the precision equipment industry and on governmental procurement programs—evolves in the world of security conventions (such as the World Security Fair, where hundreds of companies show their products each year).

People: Who are the experts?

Before the Second World War FDEs were self-taught individuals involved professionally with handwriting on a daily basis, such as penmanship teachers, bank clerks, and typographers. A few, like Edmond Locard or Archibald Reiss (1875–1929), were polymaths, criminologists officiating in all forensic areas. Locard was also something of a “gentleman criminologist,” true mirror of “gentleman burglars” like Arsène Lupin: a man of independent means, he never received a salary for his forty years of service to the French police, in his own words “nothing being of greater value to me as my liberty.” [Locard 1957: 27–28, Mazéret 2006: 85]
forensic laboratories or with established private experts, and since more recently they can take FD specialization courses as part of academic forensic science degrees.\(^1\) Today the duration is two or three years and certifications are issued by professional organizations and universities;\(^2\) laboratories are encouraged to obtain accreditations.\(^3\) The issue of a solid scientific and standardized curriculum has still to be solved.\(^4\) For examples see Fact sheet “Example curricula.”\(^5\)

**Gender gap** — Notice has to be taken about the gender demographics within the profession.\(^6\) FD is currently male dominated and thus contrasts with the overall situation in forensics, where female overrepresentation makes it one of the most popular disciplines among women. The situation is mirrored in the abysmal participation levels of women in computer science compared to that of science and engineering in general, which lately achieved parity. These gender gaps exist both during the educational stage for students and in the professional life. With the present disaffection for scientific careers the trend is likely to deepen. While gender disparity does affect the kind of technologies being produced, what, if any, impact the paradoxical demographics of FD and computing has, is unknown.\(^7\)

In practice collaborative projects are likely to encounter a much greater variety of gender distributions than suggested by the abstracted mean values mentioned above, due to the high variability of demographics across cohorts. Organizational, economical, and political circumstances can drastically and abruptly affect the number of FDEs in laboratories, both public and private. Also, among the computer science students participating in FD projects, percentages of women are different at master and doctorate levels. More fundamentally, gender demographics in computing vary considerably across cultures, making the combined gender composition of a team of FDEs and computer scientists less predictable.

**Objects: What is a forensic document?**

Although the handwritten message on paper is a popular image of objects examined by FDEs (think threat letters and suicide notes), significant time is devoted to other document types: ► identity documents (passports, driver’s licenses...); ► legal documents (wills, contracts, diplomas...); ► legal

---

\(^3\)— Standards ISO 17025, “General requirements for the competence of testing and calibration laboratories,” and ISO 17020, “General criteria for the operation of various types of bodies performing inspection.” Maxwell and Morris 2011; Melson et al. 2009 [laboratories], Schiffer and Stauf er 2009 [organizations].  
\(^5\)—See p. 101.  
\(^6\)—Figures and references are provided in “Gender demographics,” p. 105.  
\(^7\)—But consider the psychology of programmers: e.g., Tognazzini 1992: 93–113 [survey at Apple], Weinberg 1971: 141–159 [caveats on interpreting surveys].

**Expert Bytes: Computer Expertise in Forensic Documents - Players, Needs, Resources and Pitfalls**

Author: Vlad Atanasiu  
Copyright 2014 Taylor and Francis, LLC  
http://www.crcpress.com/product/isbn/9781466591905
tender (banknotes, checks...); ► graffiti and seals; ► digital documents (altered PDFs, images...; usually part of digital forensics 1). In practice virtually any inscription, in any media, is a potential FD.

These documents are characterized by a great diversity of visual shapes; technologies and materials; contexts, contents, and functions; conditions of collection, access, handling, and storage—but they are all inscriptions. All are also part of the work of FDEs and potentially represented as digital images. The main categories as reflected in practical FD work arrangements (personnel expertise, literature classification, financial, and material resource allocation) are optical patterns (handwriting, machine writing, signature, drawings...) and physical traces (ink, printers, paper...). FD typologies can serve to select research project subjects. Note how the forensic document extends beyond the materiality of the written object to include the larger context of its production and origins (its history), as well as the biological and sociocultural characteristics of the writer. For terminology and typology, see Fact sheet “Diverse goals + aspects.” 2

Goals: Why are forensic documents examined?

From a cryptographic perspective, forensic expertise is a process applied to a system of two disentangled parts of a single entity (agent and trace) and the link between them. The goal of this expertise is to question each of these three elements, through: ► identification: given some traces, answer the question “Who is the authoring agent?” ► verification (forensics) or authentication (biometrics, security documents): given a purported link between agent and trace, is the link genuine? 3 ► recovery: recover illegible or missing traces (reading of erased writing or charred documents...); ► intelligence: what can the traces tell us about the behavior driving the agent and about its social network (analysis of the crime phenomenon, respectively criminal intelligence)? ► support: tasks in support of the aforementioned goals (computerized document management, physical analysis, imaging, establishment of reference datasets, quantification of expert opinion...).

Agent, trace, and link are a terminology that was kept general for a reason: it can be embodied in any of the expertise objects listed in the preceding section. For example, an agent usually refers to an individual, but can equally well signify a typewriter that has to be identified.

Conditions: How does forensic document expertise operate?

It is common to hear FDEs comment that developed forensic software or quantitative methods are irrelevant to their work. For example, many writer identification techniques assume the existence of a substantial amount of...
writing samples from both crime scene and suspects, while in reality many forensic documents are just a couple of lines long, if not just a few words. Knowing the object and goals of FD as described above must be complemented with an intimate understanding of the operating conditions. These physical, technical, organizational, social, and psychological constraints are also issues that FDEs have to address, and ultimately the software and analytical methods too if they are to be of any real use. Operating conditions are indeed part of the forensic document—even if the continuity between the two is materially invisible—because they cannot exist independently.

Expertise circumstances are volatile, varying in time and between cases under consideration, laboratories, and countries. A few of them should be mentioned to show their impact on possible computer science projects and help clarify the expectations of the involved parties. It is noteworthy that they represent a class of computational FD solutions by themselves, on par with those dedicated to the core FD goals.

Software marginality — The logo of the Association of Forensic Document Examiners (AFDE), depicting a microscope, formally reflects what FDEs perceive as their primary tool of trade: “The most important tool for the forensic document examiner has been, is, and probably always will be, the optical stereomicroscope.” Hardware-based analyses are preponderant in FD, as the number of publications concerning them suggests. Software use by FDEs is marginal—for handwriting expertise, for example, the active systems that exist (the European and United Stated FISH) are restricted to governments, while the few commercial and academic products are prototypes or not used. The introductory text to the first forensic signature competition, in which the Netherlands Forensic Institute (NFI) explicitly states the goal of its sponsoring to be the acquisition of a signature expertise software for active casework, is one of the signals in recent years signifying the slow turn toward information technologies initiated by the FD profession itself. This is not surprising since the training of human experts consists, after all, in creating a biological pattern recognizer.

Focus on forgeries — Disguised handwriting and signatures are a topic example needing the experience of an FDE to be appreciated as a worthy computer research subject. Disguise cases are not that infrequent to neglect them, but there are very few relevant computational studies. In any case it is an intellectually interesting topic, fusing a number of areas, including psychology and biokinematics (as a historical aside, Alphonse Bertillon (1853–1914), a founding figure of the scientific method in forensics, erroneously conjectured autoforgery in the Dreyfus affair).
Applications variety — The wide array of forensic document types demands an equally large spectrum of expertise and resources: training, datasets, methods, tools, and so forth. Even when restricted to a single topic such as handwriting, a single software cannot process equally well all possible circumstances where the topic appears. Understanding and explaining to FDEs the conditions under which the software performs optimally is thus necessary. Variety, nevertheless, is also a boon for developers, providing many research and development opportunities.

Topic inconstancy — In addition to the specialization induced by forensic documents, they are also characterized by sometimes fleeting interests born outside the field. Anthrax was a relatively obscure research subject until the 2001 terrorist attacks in the United States — and subsequently faded back to its previous fate. More to the point of FD, research into Arabic handwriting has also — apparently for a longer period — boomed since the same fateful year 2001. Here we talk of a research body matured over the years, but how much time does one have to develop software for a reliable understanding of the conditions of handwriting with a victim’s blood on wine cellar doors of the French Riviera? How far can an FDE expect to find computerized help in such rare cases? Time-consuming scientific research also squares badly with a CSI TV-series-fed public expecting forensics to be “sexy, fast and remarkably certain.” The popular image of forensics is not innocent — one way or the other it does have a bearing on the judicial process.

Time limitations — The issue of FDEs having a limited time to devote to specific document types is compounded by many of these documents not being available for later consultation once the expertise is performed. After examination, forensic laboratories return the documents to courts, lawyers, private persons, or law enforcement agencies, and digital or analog copies are not necessarily made for the lab’s own archives. Evidently this influences the expertise range and performance of FDEs (fleeting memories, limited teaching material) and the ability to develop meaningful support software.

Postfactum expertise — Typically FDEs are consulted after crimes have been committed (serial murder cases and antiterrorism are some of the exceptions). In this respect their work contrasts with that of signature biometric access control and security documents validation which happen in real time given the speed and volume requirements critical to such transactions. This characteristic has far-reaching implications on the nature of techniques that can be used in an offline setting. For example, code optimization, bandwidth, and detail of analysis, become lesser concerns.

Cultural specificities — Along time, space is also an FD factor: some document types or inquiry topics are culturally specific. Seals have become of interest to the Western FD only for the examination of official documents,
but metal and stone seals still are the dominant means of personal identification in Japan and Taiwan (former Japanese colony until 1945), as they were throughout Eurasia for most of its history. The contribution of Japan to computational research on Western-style signatures is therefore understandably minimal (less obvious is the disconnection from forensic computational handwriting analysis in general). Also, handwriting written with a brush is common in the Far East, and accordingly, many computer methods for brush synthesis and analysis have been developed in China, which has a vibrant calligraphic culture.

**Tailored ergonomics** — As a social construct FD is affected by the training of its practitioners and requires adapted software. As the typical FDE educational curriculum is not science oriented, in particular computer science and statistics, forensic technologies developed in these areas must make an effort to be accessible to their final users. Appropriate computer interfaces, terminology, and documentation are some of the topics of concern.

**Socioprofessional priorities** — Sociologists working with members of police forces have reported being regarded as strangers because it was not clear what they were “doing,” the nature and purpose of academic work being alien to the practically oriented culture of the law enforcement. Academic computer scientists too can fall into this trap. Without proper communication it might not be readily understood why it is important to them to concentrate on solving abstract computational issues and publish in specialized journals, rather than delivering a working software.

**Organizational considerations** — Organizational issues can affect the development of certain FD computational resources. For example, software for detecting forgeries of Euro banknotes can be developed to read the unique serial numbers and check their validity according to a publicly known formula. However, the exhaustive specifications of security features of banknotes and official documents are best known to the issuing institutions. When the development of software methods depends on access to datasets and specifications (e.g., for machine learning purposes), co-opting the goodwill of the relevant institutions is a prerequisite to success. Fortunately, the FD community is quite transparent about its dealings and open to scientific collaborations. Such an attitude might be different in the realms of security documents or cryptography, where nondisclosure is indeed the rule or at least a passionately controversial topic.

**Legal constraints** — The laws governing FD work also have to be taken into account by researchers since they can affect not only the project’s management, but the very nature of the technologies to be developed. Consider for an instant the peculiarities and variety of software that need to be imagined and implemented (anonymization tools, network security…) to build an

---

1—Fleming 2010: 144.  2—Deroche and Prieur 2003.  3—Van Renesse’s handbook on optical document security, for example, opens in each new edition with an evolving discussion to the appropriateness of publishing such a book, to which, indeed, some invited experts declined to contribute on moral grounds [Renesse 1998: xvi–xxvii, 2005: xii–xv].

**Expert Bytes: Computer Expertise in Forensic Documents - Players, Needs, Resources and Pitfalls**

Author: Vlad Atanasiu
Copyright 2014 Taylor and Francis, LLC
http://www.crcpress.com/product/isbn/9781466591905
international networked forensic handwriting database that accommodates the laws pertaining to cross-border dataset sharing. More generally, the evolution of the admissibility of handwriting expertise in courts, especially under the Daubert ruling of 1993 in the United States that sets conformance criteria, has initiated a research for a better, scientifically plausible FD. Development of FD practice standards and quantitative methods to evaluate the strength of evidence are two of the more visible results of these efforts.  

**Judicial use** — Finally, computer scientists have to remember that a forensic expert occasionally has to witness in courts. This person therefore needs technologies that can be reasonably well understood and easy to explain. Ultimately FD is about justice and affects the life of individuals — software needs to be ethical.  

The neutrality of the expert witness is of particular interest to the adversarial setting of the common law justice systems, mostly Anglo-Saxon. Because experts are hired by the conflicting parties rather than appointed by the judge as in the inquisitorial tradition of continental law of most of Europe, they become more advocates than impartial auxiliaries. Recognizing the issue of a science being bended so as to agree with the desired outcome of a case, the Panel on Statistical Assessments as Evidence in the Courts sponsored by the US National Science Foundation issued in 1989 recommendations for developing standards to preserve the ethical integrity and scientific independence of expert witnesses. Interestingly, the impact of the specificities of a judicial system on the state of forensics resurfaced 20 years later, in the National Science Foundation report of 2009, this time focusing on the too close relation between forensic laboratories and law enforcement agencies.

---

1—For a glance at the legal aspects of forensics in the United States see Houck and Siegel 2010: 579–611.  
2—The confusing explanations and condescending attitude of Bertillon as a handwriting expert during the Dreyfus trials made him a laughing stock of the public. Here is how the New York Times correspondent related the court proceedings: “The witness began by saying that only intelligent men could follow his explanations, and the court was half emptied as the audience, after smiling audibly at his extraordinary words and expressions, soon became bored and went out. […] ¶ The courtroom presented a curious scene while M. Bertillon, whom the Dreyfusards, in their most indulgent moments, describe as a ‘dangerous maniac,’ spend the remaining hours of the session in explaining, in unintelligible terms, his ‘infallible system’ of proving Dreyfus was the author of the bordereau. The majority of the public, however, utterly unable to comprehend M. Bertillon’s theories, had left the courtroom. Even ‘La Dame Blanche’ (the white lady) abandoned her post. ¶ In the meanwhile, M. Bertillon, with gestures and in the shrill, pitched voice of a quack at a country fair, continued his monologue, producing every minute some fresh paper covered with wonderful hieroglyphics, copies of which he presented to the Judges, who, with an expression of owllike wisdom, carefully examined them, their heads clustered together, their eyes gazing on the long, wide strips of paper, while M. Bertillon leaned over their table trying to explain his mystifying diagrams, which were afterwards passed to MM. Labori and Demange, who, however, apparently, did not derive much profit from their perusal. ¶ Dreyfus gazed at the scene with a look of stupefaction.” [NYT 1899]  
3—See the ethics codes of several computing associations in Johnson and Snapper 1985: 14–42, and a philosopher’s take on their merits: “the whole notion of an organized professional ethics is an absurdity—intellectual and moral.” [Ladd 1985: 8]  
Stress — Forensic science is not all science, it is also social performance, as the forensic etymon spells it out. Its judicial use generates psychological stress, fires up egos, and puts reputations at stake. FDEs have to contend with pressure from the laboratory hierarchy or their customers to deliver in time and perhaps in their favor; court appearances can be daunting, adverse parties questioning with inquisitorial fervor every bit of the FDE’s qualifications and logic, eloquence and assertiveness being paramount; the media’s lights and public opinion can at times attain properly hysterical proportions; and not last, the importance of the case can be a crushing moral burden.\(^1\) In all this the FDE has to maintain professional integrity and defend her or his expertise, maybe shaped by the use of software. Which opens the possibility of the software’s creator being summoned in court and subjected to the same grueling experience as just canvassed for the FDE.\(^2\)

---

1—To internalize this physiological state, readings in history, social science, and history of science and technology, as well as court transcripts are recommended: Moenssens 2009 [description of the expert cross-examination procedure], Zajac and Hayne 2009 [intimidating techniques learned by lawyers, impact of cross-examination on children], Cole 2009 [on the right and duty of scientists to intervene in judicial debates of scientific quality of forensics], Saks 2003b [a scholar’s deposition], Fisher 2008: 182–217 [the Ramsey murder case], Wikipedia 2012a [Dreyfus affair], Stone 1984: 96 [how the performance of psychiatrists in court can influence their profession].  

2—What happens then see in Lynch and Cole 2005.