Chapter 12
On Complex Crimes and Digital Forensics

Martin S. Olivier
University of Pretoria, South Africa

ABSTRACT
Science provides the basis for truth claims in forensics. Very little research has been done to explore the scientific basis of digital forensics. The work that has been done vary widely in what they propose; in most cases it is unclear how the philosophical remarks about such forensic science apply to digital forensics practice, or that the practical suggestions are a sufficient basis to claim that practice based on them is scientific. This chapter provides an initial exploration of the potential of decision problems from the field of algorithmics to form this scientific basis. There is no doubt that decision problems operate in the scientific domain and decision problems look similar to hypotheses to be of immediate practical use. The chapter suggests that, if decision problems are used in this manner, it is clear that current digital forensics have only scratched the surface of what is possible. Probabilistic complexity classes, for example, offer interesting possibilities for performing complex tests in relatively short times, with known error rates. Using decision problems as a demarcation criterion makes it possible to distinguish between digital forensic science (or simply digital forensics) and digital forensic craft, which should be called digital investigative technique or some other suitable term that does not imply that its use leads to scientific truths.

INTRODUCTION
Forensics entails the use of science to determine matters of fact where such facts are required to settle disputes (for example, in courts of law) or to determine the root cause of an event of interest. Forensics employs the notion that scientific knowledge is true and hence a good basis to settle such disputes and/or determine causes. Digital forensics is that branch of forensics that studies evidence that exists is digital form.

In order to make such truth claims forensics has to be ‘scientific’. In some cases this is emphasised by using the term forensic science, which in this paper will be deemed to be synonymous with the term forensics. The notion of science (as well as the notion of truth) has been the subject of deep philosophical reflection over centuries; so much has been said that a paper that ultimately intends to deal with a small fraction of forensic science cannot hope to do justice to.

DOI: 10.4018/978-1-4666-6158-5.ch012
The obvious question then is what is the nature of digital forensic science or, with the same meaning, the science that underlies digital forensics? Cohen (2012) is the only author who has provided a coherent answer to this question by describing an information physics — ‘natural laws’ that apply to information and can be used as the basis for more complex truth claims. However, it is not yet clear that it is possible to always relate the behaviour of a complex system to truths about bits and related matters—see, for example, Hofstadter’s argument (1979) that a complex system may be more than the mere sum of its parts and may exhibit characteristics that are not present in the parts.

A recent newspaper story (Koppl & Ferraro, 2012) provides some insight on what may go wrong if we rely on digital forensics that cannot be trusted—it may negatively affect innocent people. However, simply discarding digital forensics because of a lack of trust turns the cyberworld into a safe haven for criminals who can exploit others without fear of being caught. Clearly a digital forensics is required that maximises the chances that the guilt of the guilty can be proven, and that will ideally never implicate an innocent party. If these requirements are met the inhabitants of cyberspace can proceed with trust even in those cases where the proactive security mechanisms fail. Note that this problem is not only present in digital forensics; other branches of forensics have also failed because they used junk science or pseudoscience (Giannelli, 2007; Saks & Faigman, 2008). Regarding digital forensics, Caloyannides (2006) boldly declares that “It is important for judges and juries to be highly sceptical of any claims by prosecution that digital ‘evidence’ proves anything at all.”

This paper will examine the suitability of algorithmics or algorithmic complexity theory to form the basis of digital forensics. The justification of positing algorithmics as this basis is deferred to later in the paper when required underlying issues have been discussed. From the outset it is important to note that the paper distinguishes between expert testimony and forensics. In many jurisdictions forensic evidence can only be introduced in a court case by means of expert testimony. However, not all expert testimony is based on forensics. Consider, for example, the medical doctor who testifies as an expert about the current standard of care for some ailment. This testimony will be partly based on medical training (including continuing education), partly on professional observation of what colleagues do, partly by standards that may have been published by national and international bodies and partly by local conditions (such as affordability of various treatment options).

Clearly such testimony from an expert may be invaluable in a case where it is required. However, such evidence will not be classified as scientific evidence. In particular is this witness not basing evidence on forensic science. The remainder of the paper is structured as follows. The next section reviews some characteristics of science, forensic science and expert testimony to provide context for the exploration of digital forensic science that follows. Section 3 initiates this exploration by discussing two simple (and common) scenarios at length. Section 4 uses these scenarios, the notion of decision problems and expectations about digital forensic science from the literature to begin to develop a theory of digital forensics that can claim to be scientific. Section 5 briefly mentions some competing theories. Section 6 concludes the paper.

**ON SCIENCE, FORENSIC SCIENCE, AND EXPERT TESTIMONY**

As noted earlier the intention of the current paper is not to explore the notion of science in depth. In the philosophy of science the following three landmarks are most important for the purposes of this paper. Firstly, in the period before the Second World War a group known as the Vienna Circle developed the notion of logical positivism. Ac-