A Comparative Study of Teaching Forensics at a University Degree Level

Philip Anderson[1], Maximillian Dornseif[2], Felix C. Freiling[2], Thorsten Holz[2], Alastair Irons[1], Christopher Laing[1], and Martin Mink[3]

[1] School of Computing, Engineering and Information Sciences, Northumbria University, Newcastle upon Tyne, NE2 1XE, U.K.
[2] Department of Computer Science, Universiy of Mannheim, D-68131 Mannheim, Germany
[3] Department of Computer Science, RWTH Aachen University, D-52056 Aachen, Germany

Abstract. Computer forensics is a relatively young University discipline which has developed strongly in the United States and the United Kingdom but is still in its infancy in continental Europe. The national programmes and courses offered therefore differ in many ways. We report on two recently established degree programmes from two European countries: Great Britain and Germany. We present and compare the design of both programmes and conclude that they cover two complementary and orthogonal aspects of computer forensics education: (a) rigorous practical skills and (b) competence for fundamental research discoveries.

1 Introduction

In recent years, computing technology and computer systems have experienced dramatic growth. The growth in the number of systems (communications, information systems, Internet systems and e-commerce), the advances in the functionality and the usability of systems have provided opportunities for malicious users to exploit insecure and non-robust systems and attempt to conceal their activities. As part of the misuse of systems, perpetrators normally make attempts to cover their tracks and destroy evidence of their actions. The ability to determine where cybercrime may have taken place and the resultant requirement to examine the cybertrail have raised the need to develop specialists in *computer forensics* – a set of practitioners who have the methods, skills and techniques to preserve, identify, extract, analyse and document the evidence stored in the form of digitally encoded information.

The skills required from computer forensics experts are many: (a) They must be good computer scientists trained to deal with various hard- and software systems. (b) They must be educated in law to be able to assess and sort out relevant evidence. (c) They must be trained in the principles of forensic science, obeying the principles of sound and complete documentation of their actions. (d) Last but not least, they must be able to judge their actions in the context of psychological stress and possible own criminal activity or personal gain, making it necessary

to reflect deep issues of professional ethics. Allthough different approaches have been reported [4], due to this large spectrum of skills, graduate level education (at a University degree level) is commonly regarded as the best way to teach computer forensics.

Computer forensics is a relatively young University discipline which has developed strongly in the United States and the United Kingdom but is still in its infancy in continental Europe. The national programmes and courses offered therefore differ in many ways. Unlike traditional forensic science, which is almost always practised within a single national law context, computer crime and therefore computer forensics has a global aspect because computer crime often involves global computer and telecommunications networks like the Internet. National standards in computer forensics education are therefore only of limited value.

The aim of this paper is to approach the question of possible international standards in computer forensics education by comparing rather different University degree computer forensics curricula from two countries, the United Kingdom and Germany. The British case is a full BSc Honours programme in Computer Forensics at Northumbria University while the German case is an area of specialization within a general Computer Science Diploma degree programme at RWTH Aachen University, with which until recently all German authors were affiliated.

Both programmes are running for roughly two years so they cannot be compared by their output (in terms of students) yet. In this paper we therefore compare the *design* of these programmes, which — as the discussion will show — can be regarded as prototypical in two complementary and orthogonal aspects: (a) rigorous practical skills and (b) competence for fundamental research discoveries. Roughly speaking, the British case educates students in using standard forensic tools whereas the German case is more aimed at training students to build and improve standard tools.

The paper first presents the British case in Section 2 followed by a presentation of the German case in Section 3. Section 4 compares both cases and draws some conclusions.

2 The British Case

The programme at Northumbria University is an example of a UK computer forensics programme and as such has to comply with Higher Education Funding Council for England (HEFCE) regulations, the National Qualifications Framework, the Quality Assurance Agency (QAA) Computing Benchmark Statement and the British Computer Society (professional body for computing in the UK) expectations. In addition the programme at Northumbria has embedded the Association of Chief Police Officers (ACPO) guidelines for handling digital evidence [2] in the design of the programme. As yet there are no specific regulations from forensic science professional bodies that are applicable for computer forensics programmes, but is expected that this will change in the next few years. Al-

ready the Council for the Registration of Forensics Practitioners (CRFP) has begun to allow computer forensics practitioners to apply for individual registration [3], and is expected that bodies such as the CRFP will begin to move towards accrediting computer forensics programmes.

2.1 Motivation

There were a number of drivers for developing the programme in computer forensics at Northumbria. The topic, along with computer crime, had been included in a compulsory final year computer ethics module; according to student feedback these topics were very popular. Research interests of a number of members of academic staff in the School were centred on computer forensics and a growing body of knowledge was evolving in the School. Feedback from employer groups suggested that the subject would be popular. Senior members of the School were involved with the *North East Fraud Forum* and computer forensics was an area of growing interest in this group. Pragmatically the School also wanted to attract students and popular exposure on TV and in the media helped raise the profile of the computer forensics and as such raised popularity with potential students.

2.2 Programme Philosophy

The BSc (Honours) Computer Forensics programme addresses the rapidly emerging need of Police forces, security agencies, commercial organisations specialising in computer forensics and as part of larger organisations (where there is the need to carry out internal investigations) for skilled professionals in the developing area of computer forensics. The essence of the programme focuses on the principles of evidential integrity, evidential continuity and the challenges of dealing with digital evidence. The programme adopts the philosophy of providing an educational programme which addresses the fundamental and underpinning principles of Computing as designated in the QAA Computing Benchmark, whilst focussing on the theoretical, professional, technical, legal and social aspects and concepts of computer forensics.

The programme provides students with the knowledge to professionally, systematically and impartially approach the preservation and extraction of all relevant digital evidence from computers, computer systems and computer networks (including the Internet). Further, the programme prepares students for practice in the discipline of computer forensics using the principles defined by the Association of Chief Police Officers [2].

The content of this programme and the skills and techniques developed in the programme are potentially damaging if used maliciously. Consequently, the teaching staff emphasise the professional expectations of students working in this domain, as well as stressing the students ethical and moral responsibilities to themselves and others, including the School and the University.

2.3 Curriculum Design

The programme was designed, in collaboration with practitioners, to address the skills, techniques and theoretical requirements for graduates to work in the field of computer forensics. The programme also exposes students to computer forensics cases through analysis of historical cases (taking into account confidentiality, anonymity and other ethical considerations), hypothetical case studies and cases made available in the public domain.

The design of this degree expressly supports the employability of its graduates: the choice of skill and knowledge areas, tools, techniques and methods has been made to ensure students are immediately useful to employers, both at the placement and at the graduate stage. Industry practice and subject benchmarking strongly influenced the design of the programme, and hence the programme content will continue to evolve in line with developments in the industry and in the subject as an academic discipline.

Key transferable and interpersonal skills are developed throughout the programme, and students are encouraged to reflect on this process via their Personal Development Plans. Through formative and summative coursework, students develop and apply computational, communication and team-working skills. The ability to work effectively as an individual, both as a student and as a practitioner, is a critical skill developed throughout the programme. Learning independently, managing others and oneself on project tasks, evaluating and reflecting upon practitioner experience are all essential skills of the computing professional, which the taught modules help to develop, they provide students with opportunities to contribute towards their personal development planning.

The programme has been designed to introduce computer forensics in the first year, increasing the coverage in the second year and almost the full final year given to computer forensics. Figure 1 depicts the programme structure. For lack of space we cannot enumerate the contents of all courses, however areas marked with grey indicate the proportion of the programme given to computer forensics. A unit point in Figure 1 measures the effort of about 15 working hours. This roughly corresponds to half a standardized European Credit Point (ECTS).

The programme includes a placement year between second and final year. The placement experience significantly enhances the employability opportunities of graduates. Through careful support of the student and employer, and subsequent supervision of the placement activities, the placement period becomes highly valued preparation for the final year of study and graduate employment. As well as developing specific technical skills and techniques students obtain invaluable experience in developing their self-confidence and maturity, and greatly enhancing their academic and employment prospects.

2.4 Laboratory Facilities

In order to teach computer forensics in as realistic a setting as possible a computer forensics laboratory was commissioned to provide students with opportunities to develop practical skills and techniques using computer forensics tools

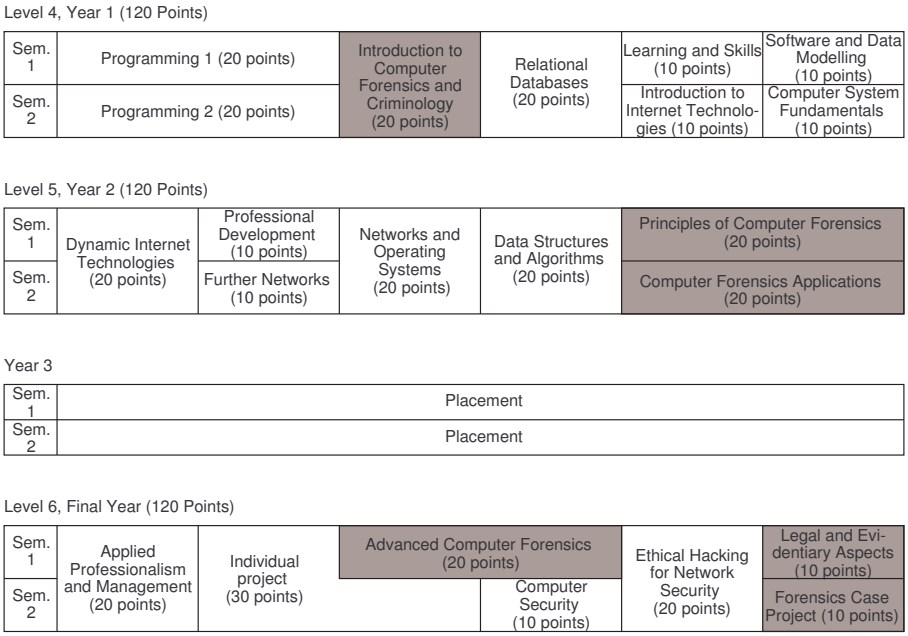

Fig. 1. Programme Structure Diagram: BSc (Honours) Computer Forensics at Northumbria University.

in a safe and secure environment. Specific computer forensic specific software and hardware requirements were included in the specification of the laboratory. Although the laboratory is networked (to facilitate network forensics) the laboratory is not connected to the University network. Since the computer forensics laboratory acts as a base room for the computer forensics students, it also helps to build a peer support culture and a cohort identity.

2.5 Ethics

There is a significant challenge in teaching ethical awareness and embedding the principles of computer ethics into the teaching of computer forensics. There is a need to make students aware of the potential for misuse of computer forensics tools and techniques as well as the need to instil ethical and professional behaviour into computer forensics practices. It should be noted that a condition of the validation process, was how ethical issues (including computer ethics) would be included within the computer forensic degree.

In the computer forensics programme at Northumbria ethical issues are introduced early in the programme. Students are introduced to computer ethics in their induction week and throughout the 1st year computer forensics module. Early in the module students are given the task of develop their own Ethical Code for Computer Forensics.

2.6 Inter Disciplinary Considerations

Armstrong and Jayaratna [1] argue that computer forensics requires not only specialist computer knowledge, but also a multi-disciplinary background and understanding, drawing on principles from forensic science, criminology, law, mathematics, and business as well as from computer science. Consequently, the programme at Northumbria is closely aligned to other disciplines, for example, a first year module has input from the Universitys School of Applied Sciences forensic scientists (principles of forensic science) and the Universitys School of Arts and Social Sciences criminologists (criminal justice systems and criminal motivation). While a final year module on Legal and Evidentiary Aspects of Computer Forensics includes inputs from the Universitys School of Law who act as barristers for the defence and prosecution in examining and cross examining computer forensics students as they take on the role of an expert witnesses.

2.7 Employer Links

Practitioners have a significant impact on all Northumbrias degree provision through input to the development of the curriculum, providing expert knowledge to programmes through presentations and case studies and providing placement and employment opportunities.

In this case, computer forensics practitioners participated as part of the computer forensics programme validation process. In addition colleagues from police forces (National High Tech Crime Unit, Northumbria Police, West Midlands Police), Computer Forensics Providers (Sapphire Technologies, DNS), Computer Forensics Software Developers (Guidance Software), Legal Firms (Dickinson Dees), Computing Consultancies (Price Waterhouse Coopers), Financial Institutions (Skipton Building Society, Northern Rock), kindly provided seminars and presentations to the computer forensics students. These sessions have helped in developing relationships with employers and have given students a practitioner view of the theoretical and practical aspects taught on the programme. It should be noted, that as part of the ongoing review of the programme there is an Employer Liaison Group, which acts as an informal network between employers and academics, but also between employers.

3 The German Case

3.1 Motivation

Unlike the United Kingdom, in other countries of continental Europe like Germany graduate programmes specialized in computer forensics are rare. In fact, the authors are unaware of any specialized graduate level programme in Germany to date. Several Universities of applied sciences ("Fachhochschulen", they do not offer PhD programmes) offer computer forensics courses as part of a specialized BSc or MBA programme, but none has a programme entirely devoted to computer forensics. The situation is not much different at the level of Universities which offer PhD degrees.

Interest in computer forensics let several researchers at RWTH Aachen University develop a curriculum specialized in acquiring and evaluating digital evidence. Due to restricted resources, developing a new degree programme specialized in forensics was not possible. However, the German University system offers educators a lot of freedom in what and how lectures are offered. Students are also very free in their choices of subjects at the starting from their third year within a Diploma programme. So we offered the curriculum as a so called "area of specialization" within a traditional Computer Science Diploma programme.

3.2 Overview

The two-semester university degree curriculum which is offered at RWTH Aachen University is depicted in Figure 2. We briefly describe the scope of the individual courses with particular attention to the course on Computer Forensics. The unit used in the explanation have been calculated to be the same unit as in the British case.

- The first semester has three elements: (1) a lecture on *basic concepts of computer security* (20 points), (2) a lecture on *computer forensics* (12 points), and (3) a *research seminar* (6 points) on current trends in computer security where students give a presentation.
- The second semester consists of (1) a lecture on *security failures in web applications* (10 points) and (2) an extensive *practical lab* (20 points) in which students apply offensive and defensive techniques within an isolated test network. The final part of the semester is a *Summerschool* (20 points) in which advanced attacking techniques are trained and analysed.

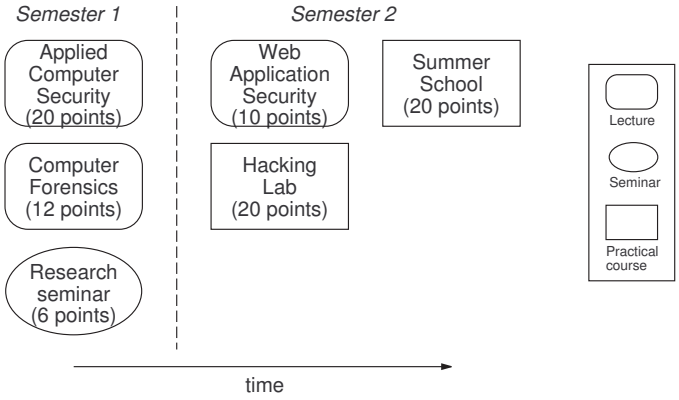

Fig. 2. IT security curriculum at RWTH Aachen University

The lecture *Applied Computer Security* is a standard lecture (4 lecture hours per week) in which basic concepts of computer security are explained to the

audience. After discussing basic terminology issues, the course first looks at the security concepts which are present in a standalone UNIX or Linux PC (authentication techniques, access control, cryptography basics, backups and physical security, among other). The second part of the course covers network and Internet security issues, e.g., securing TCP and UDP services, network based authentication systems, network filesystems and secure programming techniques. Whenever suitable, common vulnerabilities and attack techniques are discussed to focus on weaknesses of current technologies. For example, dictionary attacks on passwords are discussed in the lecture on password-based authentication, or buffer-overflow attacks are discussed in the context of secure programming techniques. This lecture is meant as a "mind opener" to a broad range of aspects of computer security.

Common Failures in Internet Applications (or "How Webservers get 0wned") is a lecture designed to teach how insecure Web applications can be broken. In a case-study approach problems are shown that arise from using web applications such as Webserver (i.e. HTTP) or Mailserver (i.e. SMTP), and helpers as PHP, HTTP cookies and authentication (e.g. SQL injection, cross site scripting, session highjacking, tampering of hidden HTTP fields). Finding vulnerable services by using search machines (e.g. database or printer administration webpages accessible via the Internet) and available tools (e.g. application proxies) are demonstrated to the audience.

The practical course *Hacking Lab* gives students the opportunity to get practical experience of real life security in a controlled environment. As an administrator and as a hacker they get to know both sides of security (defense and attack), making them aware of security problems and enabling them to develop advanced techniques for defense. The course has evolved over time: the first time there were only few instructions given and students had to install the (operating) systems themselves, over more instructions and some work sheets, to bi-monthly work sheets and aspects of *capture-the-flag* (CTF) contests in the current course. In all courses students work in teams. Each team administrates several computers, and then on one hand tries to secure their own systems, on the other hand to find vulnerabilities in the other teams' systems. The computers used are inside an isolated test network, giving the students the possibility to try attacks and getting attacked without implications to the outside (Internet, Intranet).

In the two or three week *Summerschool "Applied IT Security"* students are given the opportunity to induce and study failures in security systems. Other goals are knowledge transfer and to introduce students to a scientific approach to information security. A day of the Summerschool starts with a lecture on a certain topic (e.g. forensics, malware, web applications, honeynets). In the lab session during the rest of the day participants apply the techniques learned in the lectures and develop them further. In the afternoon a so called "coffee table talk" is offered where an invited speaker presents a topic of his interest. The coffee table talks are intended to broaden the view of the participants and to get a focus on problems being faced in the real world. A day concludes with a meeting where everybody presents his work of the day.

3.3 The Computer Forensics Course

The course on computer forensics is taught with two lecture hours per week. Forensics or forensic science is the application of science to questions which are of interest to the legal system. Classic computer forensics is the gathering, interpretation and presentation of evidence found on computers. Since the aim of forensic science is to supply services to the legal system, forensics are very dependent on the kind of legal system they work with. Unfortunately nearly all literature on computer forensics originate from places where the criminal justice system stems from the common law which is very different from the German legal system. This and the fact that in the German legal community there is very little experience in using computer forensic evidence in court cases makes it difficult to give students firm guidance on how to interact with the legal system and how to testify as an expert witness in front of a court.

Therefore in our teaching we broaden the definition of computer forensics to a more computer science like definition: We understand computer forensics not primarily as a tool for the legal system, but also as a tool for understanding security. Sound engineering principles dictate a thorough analysis of failures to learn the workings of a system and avoid subsequent failures of the same kind in the future. We define computer forensics as "the attempt to reconstruct the events which lead to a security policy violation in an information security system". Thus computer forensics also includes the analysis of security incidents to learn the tools, tactics and techniques of the attackers and to gather facts needed to improve security in the future.

In light of the lack of experience of interaction between the German legal system and computer forensics and our determination to base further research on information gained via forensic analysis we put much effort in teaching students to adhere to sound scientific principles when conducting forensic examinations. Exact documentation of all steps taken and well proofed strategies to minimize the likelihood of alteration of the data gathered or the system examined lead to reproducible results meeting rigid scientific standards. Thus having a good verisimilitude of being accepted by courts and other parts of the legal system worldwide.

The computer forensics lecture and accompanying exercises aim at providing students with the necessary knowledge to understand evidence on computers at a very deep level. A big part of the lecture consists of deepening the topics from operating system and systems programming courses in areas of specific interest to forensics. These are namely networking, process management and filesystems with a strong bias to the latter. Based on a deep understanding of how relevant parts of information systems work, students learn how to extract and interpret evidence from such systems and to evaluate the validity of that information gathered. We aim at giving the students a fundamental view on how the extraction of evidence from IT systems works, enabling them to conduct forensic analysis without anything but the most basic tools. Drawing from the strong engineering skills put forward by RWTH Aachen University, our students should have the ability to develop tools they need to make their forensic analysis more

swift whenever they are in need of such tools. Ready made software tools are only covered briefly in the lectures since we assume that the fundamental knowledge acquired during the class should enable students to quickly understand the forensic tools available on the market.

The exercises accompanying the lecture aim at giving the students opportunity to experience different forensic techniques themselves. They cover a wide spectrum of tasks ranging from IP-backtracking to reverse engineering of unknown binaries. To allow students to gather first hand experience with data capture and analysis we acquired a large amount of pre-used hard disks and ask the students to image and analyse them. We also try to connect lectures and exercises to recent events, e.g. the trustworthiness of voting machines and ex-post analysis of the equipment used in an election.

3.4 Honeypots

To learn more about attack patterns and attacker behavior, the concept of *electronic decoys* is used in the area of information security. These *honeypots*, i.e., information system resources set up to be probed, attacked, and compromised, are used to learn more about the tools, tactics, and motives of the attacker community. A honeypot usually refers to an entity with certain features that make it especially attractive for attackers and can lure individuals into its vicinity.

In practice, a honeypot is commonly a conventional computer system, e.g., a commercial off-the-shelf (COTS) computer, a router, or a switch. This system has no task in the network and no regularly active users. Thus it should neither have any unusual processes nor generate any network traffic. These assumptions aid in attack detection: every interaction with the honeypot is suspicious and could point to a possibly malicious action. Hence, all network traffic to and from the honeypot is logged. In addition, system activity is recorded for later analysis.

This methodology can also provide interesting data for computer forensics. Through the wealth of data collected, these systems offer a large body of forensic evidence. Advanced tools for data analysis and data correlation help to ease the analysis process. Since successful attacks against honeypots are frequent and supposed to happen, this concept can be used to create real-world cases of computer incidents.

Honeypots can also be used to teach computer forensics. In this controlled environment, the students can learn to analyse a compromised system. Under real circumstances, they learn the methodology and common best practices to search for evidence after a compromise. Honeypots have been used as part of several courses in the curriculum at RWTH Aachen.

3.5 Ethics

During the courses – especially the ones with offensive orientation – students are introduced to the relevant paragraphs (of German law) to get to know the implications of their actions. They are made aware of ethics of hacking and advised to use proactive techniques only in the controlled environments of the courses and

to apply their knowledge for good purposes only. Overall, we have followed the approach to trust students to ethically use their knowledge of offensive security techniques. This has been rewarded by the students by a high level of discipline.

4 Comparison and Conclusions

4.1 Comparison and Discussion

Comparing the two presented cases, the British case is certainly the more mature and better-developed programme in terms of focus for industrial needs. This is mainly due to the higher amount of financial and personal resources involved in its creating as well as its development in close cooperation with industry and law enforcement agencies. It is much more focussed on Computer Forensics as the German case, as expressed by the fact that a specialized BSc degree is awarded in the end in contrast to the general diploma in computer science of the German case.

The German case at first sight seems to offer a much narrower spectrum of skills as the British case, but it should be kept in mind that the programme presented here is part (roughly 25%) of a general computer science diploma degree, which is usually considered to rank like a MSc degree. This is typical for most German computer science programmes which allow a large freedom of choice to students who have successfully passed the first 2 years of study. Its freedom is partly also a downside of the German case because supporting lectures like data communications, criminology or general forensic principles are either not mandatory or not offered at RWTH Aachen University. In contrast to the British case, the aim of the German programme is not to educate Computer Forensics practicioners but rather to educate computer scientists that can perform research in computer forensics and security. The latter finding can be substantiated by two further observations:

- The British case has a strong inter disciplinary involvement whereas the German case is almost entirely focussed on computer science (with some small law aspects).
- The British case is strongly motivated from best practices and rules of professional bodies whereas the German case is motivated by questioning standard approaches and aiming for scientific discovery.

To summarize, the two cases presented in this paper offer two complementing and orthogonal aspects of Computer Forensics education: (a) rigorous practical skills and (b) competence for fundamental research discoveries.

4.2 Conclusions

Summarizing the discussion in a basic (and simplifying) statement: The British case educates students in using standard forensic tools whereas the German case is more aimed at training students to build and improve standard tools.

Such a statement is prototypical for the differences in the aim and scope of the two implementing Universities of Northumbria and RWTH Aachen. It will be interesting how the German case develops in the future given the requirement to adhere to the Bologna process and transforming the Diploma degree programmes into a sequence of BSc and MSc programmes.

In the future it will be important to add to this theoretical study of the two programmes an empirical study on the skills and success of the students who successfully earned a degree. We are convinced that in both the German and the British case, the qualifications will allow these students an excellent placement within the job market.

References

1. C. Armstrong and N. Jayaratna. Teaching computer forensics, uniting practice with intellect. In *Proceedings of the 8th Colloquium for Information Systems Security Education*, West Point New York, June 2004.
2. Association of Chief Police Officers. Good practice guide for computer based electronic evidence, 2003. NHTCU, London.
3. C. Everett. Forensics – cred or crud. *Digital Investigation*, 2(4):237 – 238, 2005.
4. W. Harrison, G. Heuston, S. Mocas, M. Morrissey, and J. Richardson. High-tech forensics. *Comm. ACM*, 47(7):49–52, July 2004.