A Research-Led Practice-Driven Digital Forensic Curriculum to Train Next Generation of Cyber Firefighters

Syed Naqvi, Peter Sommer, Mark Josephs
Centre for Cyber Security, School of Computing and Digital Technology
Birmingham City University
Birmingham, United Kingdom
Email: [Syed.Naqvi, Peter.Sommer, Mark.Josephs]@bcu.ac.uk

***Abstract*—Lack of skilled digital forensic professionals is seriously affecting the everyday life of everyone as businesses and law enforcement are struggling to fill the bare minimum number of digital investigator positions. This skills shortage can hinder incident response, with organizations failing to put effective measures in place following a cyber-attack or to gather the digital evidence that could lead to the successful prosecution of malicious insiders and cyber-criminals. It therefore makes the connected world less secure and digital economies less reliable, affecting everyone in their ecosystems. The commercial and public sectors are looking to higher education institutions to produce quality graduates equipped to enter the digital forensics profession. This paper presents our proposed research-led, practice-driven digital forensics curriculum. The curriculum is designed to respond to employers' needs and is built on the experience of running a successful Cyber Security program at Birmingham City University in the industrial heartland of the UK. All students will take a common set of modules in the first semester, but will be given the opportunity to specialize in digital forensics in the second semester and in their summer project, enabling them to graduate with the degree of MSc Digital Forensics.**

I. Introduction

The design of the digital forensics curriculum presents a particular set of challenges [1]. The most obvious of these, common to other aspects of the teaching of cyber security, is the incredible rate of change. Students and potential employers expect that any course covers the sort of changes in IT hardware, software and social usage that they can see all around them. At the same time universities will be keen to see that the course overall meets the standards generally accepted for Masters courses and inevitably this means a process of approval by reviewing committees. A second critical feature is that while digital forensics courses often emerge from within computer science departments what is also required are skills in investigation and knowledge of the legal framework within which forensics must function.

Significant sophistication of cyber infrastructures notably during the last decade have resulted in a mushroom growth of enabling services and technologies. This technology rich paradigm has given birth to a new generation of business and social models. An ever increasing reliance of individuals, services, businesses, and governments on these cyber infrastructures is rapidly transforming them into critical infrastructures. This level of dependence of our society on cyber infrastructures implies their smooth functioning is essential for continuing with our daily activities. Well trained and well equipped Cyber watchmen have become an absolute necessity for the protection of Cyber infrastructures. The role *Cyber Firefighter* is coined by employers to describe someone who can rapidly address security incidents and threats as they appear. Their task is to maintain a vigilant lookout to discover, contain, and remediate security breaches. Moreover, solving the jigsaw puzzle of cyber incidents to demarcate the responsibilities requires not only good knowledge of the corresponding technologies but also excellent problem-solving skills and strong analytical mind-set.

We are successfully running a Cyber Security course that covers competencies outlined in the Skills Framework of the *Institute of Information Security Professionals* [2]. We are now expanding our course portfolios by designing a Digital Forensic course to reflect new market needs especially the delivery of skills highly sought by the employers. This paper presents the classical approach towards Digital Forensics and how the emerging challenges of this highly demanding sector are transforming the design, delivery and assessment requirements of this course.

In this article, which is intended for an international audience, we will seek to stick to almost-universal principles but any actual curriculum will need to refer to specific local legislation and practice. Since the authors are based in the United Kingdom we will from time to time refer, by way of illustration, to specific laws & regulations as they apply there.

II. Digital Forensics - Market Demand Analysis

Digital forensics is traditionally seen as an integral part of IT and Networks Security programmes. However, the ever increasing scope of this field has resulted in the need of designing dedicated programmes. One of the early academic papers outlining the requirements for a comprehensive computer and network forensics training and education program was [3]. In this paper, the authors partitioned the forensics discipline into the four categories of Evidence Collection, Evidence Preservation, Evidence Presentation, and Forensic Preparation. We have analysed market demands and classify them in this section.

978-1-5386-9506-7/19/$31.00 ©2019 IEEE 9–11 April, 2019 - American University in Dubai, Dubai, UAE
2019 IEEE Global Engineering Education Conference (EDUCON)

A. Technology-centric skills requirements

Digital Forensic analysts should be able to investigate cases involving contemporary technical environments. The traditional territory of digital forensics has been the exploration of hard disks containing operating systems, application programs and data files. More recently there has been the need to handle the complexities of the internals of smart phones. Network forensics covers the activities of local area networks as well as the worldwide Internet. Cloud computing and the growth of the deployment of Internet of things devices both domestically and within an industrial context are trends which are perhaps only three years old.

B. Case management skills requirements

Another trend is that the scale and scope of digital investigations is evolving with tremendous speed. There are case management challenges from dealing with the data size to the number of stakeholders involved in each investigation. Quantities of data that potentially need to be examined present problems of triage deciding which items can safely be discarded while making allowances for the possibility that a counter-party may at some point in the future say that important evidence has never been considered and is no longer available. Another aspect of the quantity of data is the search for tools and platforms that can carry out reliable automated examinations as purely manual review may prove expensive and require unacceptable periods of time. The new range of investigatory tools may need to draw in sources of evidence from many different points of origin and many different stakeholders. Also over the last several years has been the realisation of the need to deploy digital forensic tools for e-disclosure/e-discovery the requirement in both criminal prosecutions and civil litigation that counterparties should be informed of the existence of material which might assist the other side or undermine their own case.

Related to all of these is the need for discipline in managing complex cases.

C. Academic requirements

Besides employability related requirements as described in the previous subsections, there are academic requirements to ensure that academic standards are met. They are mainly governed by QAA standards in the UK [4]. Others notably certification bodies' requirements should also be met to have added-value and recognition of the programme. We aim to acquire NCSC (a part of GCHQ) certification for MSc in Digital Forensics [5] to meet domain-specific quality requirements.

D. Curriculum design requirements

This leads to a number of basic requirements in any curriculum. First there has to be coverage of core technical and practical information about the basic procedures used in digital forensics. Second, candidates must be given every opportunity to understand the detail and experience of practical work; the vast majority of digital forensic experts are practitioners. Third candidates must have a sound knowledge of research methods as the fast moving nature of the cyber world means that practitioners will always be coming across new circumstances for which there arent established standard practices they must be able to carry out the research necessary to develop new and reliable standard practices. Fourth, a sound understanding of relevant aspects of the law, including the limitations on the powers of investigators, the significance of disclosure/discovery and the courts expectation of expert evidence. Inherent in all these requirements is a fifth: the ability to write reports which enable others to follow their reasoning and which are also able to convince lawyers and the courts.

E. Our approach

To impart these skills to our students, a Digital Forensic curriculum should provide them:

- Core knowledge of the underlying concepts such as number systems, data storage formats, security models and policies, etc.
- Hands-on experience of industry-standard Digital Forensic analysis technologies to help them acquire necessary practical skills for their operational duties
- Insight into the recent adavnces in digital forensic research and practice through research-active teaching staff and industry guest speakers.
- Opportunity to develop critical thinking by giving them real-life complex problems with time-bound submission of their findings while having access to specialised investigation resources in our purpose-built Cyber Investigation facilities.
- Access to flexible learning resources and flipped curriculum to help them develop independence and problem solving techniques.

We have used a number of forums to compile a list of skillsets needed for our Digital Forensic graduates. The most obvious is to take a critical look at the current offerings from universities in the United Kingdom, the United States and elsewhere. The first UK forensic computing MSc was initiated at what was then the Royal College of military science at Shrivenham (the military part of Cranfield University) in 2001. (One of us Sommer - was the external evaluator; he then became external examiner). Since then the course and the many others that it spawned have undergone significant changes. It has also been helpful to look at the purely commercial practitioner-orientated offerings such as those from SANS and ISC2 and others which offer associated certifications. There are also a number of courses produced by particular suites of digital forensic analytic software these, while offering some guidance on general principles, are inevitably orientated towards using specific products. There have also been a series of suggestions from would-be accreditation bodies. Finally both the NSA and GCHQ have developed intense interest in encouraging the production of potential recruits by specifying their ideas of ingredients for courses.

It has also been important to garner views from potential employees both in law enforcement and in the private sector.

The process of reviewing needs in order to modify the syllabus is never ending. This contemporary skillset include:

- Good knowledge of linguistic tools to improve the efficiency of the analysis by making search words more comprehensive such as including thesaurus. This is called the use of **linguistic corpus** in running the searches.
- Better understanding of digital media storage and processing as more and more media contents are found in digital evidence nowadays and a clear understanding of **multimedia** is very helpful for the investigators.
- Use of electronic **e-Discovery** tools to deal with the scale of the digital evidence. Nowadays more and more records are produced digitally across the world and therefore the size of any investigation can easily shoot-up into terabytes even after triage. Therefore, more specific tools are needed for each stage of cyber investigations.
- Like in any other investigation, it is of prime importance to put the findings together to solve the jigsaw puzzle of the analysis. Digital Forensic analysis requires **data analytics** to solve these problems. Data analytics is a known field in Business Intelligence (famous SAS technologies). However, its scope is different in Digital Forensics where instead of business intelligence, the techniques are used for event correlations and that's why different tools are used by the investigators for this purpose.

We also need to transform classical course delivery methods where besides using flipped education, we should be using real-life case studies, developed with our industrial partners, so that students get familiarity with the real world challenges and constraints. Moreover, we have to run a series of industry seminars where practitioners are invited from law enforcement and corporate investigation units to share their experiences with the future workforce next generation of Cyber Firefighters. Most of the Digital Forensic courses are *technology-centric*, designed around the investigations of typical post-incident scenarios such as:

- Use tool *T1* to make an image of the storage drives of the suspects' computers
- Use tool *T2* to run searches on the image files
- Use tool *T3* for electronic discovery of the evidence
- Use tool *T4* for data analytics of digital records
- Use tool *T5* for events correlation to identify patterns
- ...

The students are mainly taught the post-incident scenarios with emphasis on the use of different features of the investigation technologies. The learning outcomes of these courses are generally measured in terms of the knowledge of using Digital Forensic Tools. While the knowledge of these classical tools is still useful, the onus of ***Cybercrime Investigations*** has considerably shifted from these classical combing of digital evidence to more advanced methodologies and technologies to cope with the scale and scope of modern ***Cyber Incidents*** in both preventive and reactive modes. Moreover, the learning outcomes of modern Digital Forensic courses require a better understanding of the context of investigations including regulatory compliance requirements besides the appreciation of legal issues and organisational policies.

Other factors that are influencing the learning requirements of our Digital Forensic students include advances in the networking technologies and high-speed mobile connectivity. These enabling technologies have resulted in a mushroom growth of applications and services using rich multimedia contents. This emerging trend has also impacted the traditional way of analysing a digital evidence and the knowledge of multimedia including how its data is stored in a device has become a necessity for the Digital Forensic analysts.

It is evident that classical approach of digital investigations that was confined to the scope of specific cases could not be applied to the modern investigations where a much broader and deeper understanding of the entire lifecycle of Cyber Investigations is indispensable. We have used these metrics to derive the learning requirements of our Digital Forensic students.

III. Overview of our MSc Cyber Security programme

This programme is built upon degree-level specialism and experience to prepare the student for a career in Cyber Security, including Information Security, Information Technology Security, Industrial Control System Security, and Security Incident Response. Shortage of Cybersecurity skills in the IT workforce and the need for developing new educational programmes to deliver high-quality market-oriented Cybersecurity education is the reason behind the recent 1.9B investment by UK Government. This situation reflects the high demand of Cyber Security graduates in the job market provided they are equipped with the right set of skills. This MSc Cyber Security programme is designed to tap this potential. The required quality standards are met by positioning the course contents with the UK Quality Assurance Agency (QAA) Master's Degree Characteristics Statement and GCHQ Certification scheme for Masters Degrees in Cyber Security in the view of obtaining GCHQ accreditation for this course.

This course provides future Cyber Security professionals with the knowledge and skills needed by the employers. Our strong links with industry enable us to teach the most demanding topics. Students learn state of the art technical knowledge, intellectual know-how, management capabilities and hands-on practical skills to succeed in meeting the Cyber Security challenges faced by modern organisations.

Besides full-time study, two-year part-time mode is offered to encourage those prospective students who are in employment. The part-time option will also encourage employers to support the higher-education of their employees. The programme builds upon degree-level specialism and experience to prepare the student for a career in cyber security, including Information Security, Information Technology security and Industrial Control System Security.

This course is supported by a vibrant research environment within the research Centre for Cyber Security at BCU and by

Year 1	Semester 3	Masters Project (60 credits)		
	Semester 2	Industrial Control System Security (20 credits)	Software Security & Cloud Security (20 credits)	Research Methods & Project Management (20 credits)
	Semester 1	Information Security Management (20 credits)	Digital Forensics (20 credits)	Advanced Ethical Hacking (20 credits)

Fig. 1. MSc Cyber Security (Full Time)

Year 2	Semester 3		Masters Project [60 credits]
	Semester 2	Industrial Control System Security (20 credits]	
	Semester 1	Advanced Ethical Hacking (20 credits]	
Year 1	Semester 2	Research Methods & Project Management (20 credits]	Software Security & Cloud Security (20 credits]
	Semester 1	Information Security Management (20 credits]	Digital Forensics (20 credits]

Fig. 2. MSc Cyber Security (Part Time)

traditionally strong industrial links with CISCO, Oracle, IBM, Microsoft and BT.

A. Course structure

This programme is offered both on a full-time basis and on a part-time basis. Each semester is spread over 12 teaching weeks where students have 4 hours weekly session for each module in the campus and they are required to spend on average 12 hours on self-directed learning.

1) Full-time mode: Full-time students are taught three modules of 20 credits each in Semester 1 (starting in September) and Semester 2 (starting in February). They work on their 60 credits Master project module in the summers (starting from June). The course structure for the full time students is shown in the Figure 1.

2) Part-time mode: Part-time students are taught four 20 credit modules in their first year (two in each semester) and the remaining two 20 credit modules in their second year (one in each semester). In order to complete their dissertation by the September of their second year, they are encouraged to start their research project in Semester 2 of that year.. The course structure for the full time students is shown in the Figure 2.

B. Course modules

The course has six modules of 20 credits each; and Master project module of 60 credits. Students need to pass all modules to get MSc degree in Cyber Security. These modules are detailed in this section.

1) Information Security Management: This module is designed to provide students with an in-depth knowledge and understanding of the concepts, methods, processes, tools and practices underlying good information security management. The module emphasises the use of the concept of risk, and its associated body of knowledge, to interpret security threats in an organisations context and to communicate the impact of these threats to a variety of technical and managerial stakeholders. Students develop the analytical skills to identify security gaps and evaluate business risks using appropriate qualitative and quantitative methods, and recommend cost effective mitigations comprising careful combinations of technical, procedural and administrative controls.

2) Digital Forensics: This module is designed to provide students with an understanding of forensic principles; modern techniques and support tools for analysing cyber security incidents; and current best practices for handling digital evidence in a forensically sound manner. In addition to handling incident response, students also study judicial issues, relevant national and international laws and a range of scenarios based on professional case studies illustrating issues with the admissibility of digital evidence in court. They gain hands-on skills to develop and deploy effective controls for monitoring, detecting and responding to information security incidents within the scope of criminal, civil and enterprise investigations.

3) Advanced Ethical Hacking: This module is designed to provide students with an understanding of security auditing and testing of computer networks and systems. They work in BCU purpose-built network security labs, using different tools to apply ethical hacking techniques and gain a clear understanding of cyber security breaches. They also gain an understanding of how to develop appropriate countermeasures for cyber-attacks at policy level and apply security policy enforcement rules to protect corporate assets in an organisational context.

4) Industrial Control Systems Security: This module is designed to provide students with guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). Students explore the unique performance, reliability, and safety requirements of these systems. They gain an overview of ICS and typical system topologies, identify typical threats and vulnerabilities to these systems, and discover recommended security countermeasures to mitigate the associated risks.

5) Software Security and Cloud Security: Cloud is now becoming commonplace for software deployment. This module is designed to provide students with an insight into secure software development practices, such as threat modelling, automated code review and fuzz testing. Students develop an understanding of coding bugs and design flaws that make software vulnerable to attack. They learn about vulnerability management to address software defects discovered after their deployment. They also explore the integration of emerging protocols, such as OpenID Connect over OAuth 2.0, into the

software development lifecycle so as to meet the security requirements of Cloud infrastructures.

6) Research Methods and Project Management: This module is designed to prepare students for the research project they will undertake towards the end of their Masters course. It will also equip them with knowledge and transferable skills that will help them in their subsequent career. Students explore the research literature in their discipline, research methodology and research ethics, as well as project management tools, methods and techniques. A case study approach to learning and teaching is used throughout the module and assessment, using live case studies where possible, supported by recent research and industry practice.

7) Individual Masters Project: Students undertake a sustained, in-depth and research-informed project, exploring an area of personal interest to them. In agreement with their supervisor, students select a project topic, which will take the form of a practical outcome (artefact) with accompanying contextual material. Their topic must be aligned to the cyber security programme and informed by the research strategy of the school. Students should also consider the relevance of this topic to their future academic or professional development. They are expected to work independently but will receive additional one-to-one support from their supervisor, who will be familiar with their chosen topic area.

C. Course evaluation

We have a set of evaluations to ensure the quality of each module and overall student satisfaction with the course. These evaluations take place on different occasions during the academic year. Their details are provided in this section.

1) Individual modules evaluation: We run a mid-term student survey of each module to enable the course team and management to identify and rectify any issue with the teaching. This fine grain evaluation of the course at module level provides a clearer picture of student satisfaction across the course. The student satisfaction level for MSc Cyber Security modules are in the range of 73% to 99%. These detailed evaluations are discussed in the course team meetings where student success advisors, school management, and academic services representatives are also present.

2) Overall programme evaluation: This evaluation is done through PTES (Postgraduate Taught Experience Survey), which is the postgraduate equivalent of National Student Survey (NSS). In 2018, 90% of the students who responded to the PTES were satisfied with the MSc Cyber Security course. We periodically arrange Student Feedback Forums (SFF) to keep a finger on the pulse of student satisfaction throughout their student journey.

IV. Key Features of Our Proposed MSc Digital Forensic programme

We propose a common first semester of MSc Digital Forensics programme with our MSc Cyber Security programme. This will provide better logistic arrangements for the new programme and also provide more flexibility to the students to choose the right programme with clear understanding of the scope of each of them in the first semester. Their informed decision will help them to select the programme that corresponds to their professional aspirations. They will have specialist modules in the second semester that will broadly cover the technical and legal sides of the digital forensic investigations of modern systems. The course structure for the full-time and part-time are shown in the figures 3 and 4 respectively. The specialist contents of the programme are presented in this section. They are our *Unique Selling Points (USP)* that enable us to stand out from our national competitors.

A. Legal Dimension

Any activity by a digital investigator/ digital forensics practitioner/cyber firefighter has to operate within a legal domain. Failure to do so may result in criminal laws being broken or evidence being disallowed because evidence was acquired by an abuse of process or is otherwise deemed inadmissible. There are many technical procedures which a skilled cyber firefighter can readily execute which may be disastrous for the outcome of an investigation. An understanding of the law is therefore not an optional part of a digital forensics curriculum (or for that matter a curriculum designed more broadly for cyber security professionals) but an essential feature.

In terms of learning outcomes the main constituents are: an understanding of the law as it applies to investigators, the distinction between technical and expert evidence, and the procedural and practical requirements of discovery/disclosure. At Masters level it is helpful to understand the policy issues as well as the implications for practice.

B. Law for Investigators

It must be borne in mind that almost every investigation into the contents of a computer (a term which for the purposes of this article includes not only PCs but smart phones, large corporate systems and cloud services) or the traffic between computers across a network involves intrusion into someone's private life. The law attempts to identify circumstances in which intrusions and the extent of an intrusion can be justified.

Any legal examination of a computer can only be carried out with the authorisation of the owner or, in the case of law enforcement and intelligence agencies, under a specific power. In most countries worldwide access to a computer in the absence of authorisation is a criminal offence. In the United Kingdom, more specifically, an offence under the Computer Misuse Act 1960.

Once authorisation has been secured there are still restraints on what investigators can do. Most countries subscribe to the aims of the universal declaration of human rights; the UK adoption is the Human Rights Act 1998 . Article 8 asserts the right to respect for private and family life, home and correspondence. It is a qualified right: except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention

of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. In practice that means each intrusion has to be justified on one of those grounds and tests of necessity, proportionality and care about collateral intrusion to 3rd parties must be applied. The burden of applying the tests often falls on those with technical competence the cyber firefighter.

In addition to human rights legislation many countries also have specific laws protecting personal information. In Europe there is the General Data Protection Regulation (GDPR) and the specific UK implementation is the Data Protection Act 2018 . As with the human rights act there are exceptions so permit activity by law enforcement and other agencies and other public interest issues.

The UK also makes special arrangements for employers: the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations, 2000. The tests include: to establish the existence of facts, for the purpose of preventing or detecting crime, to detect and investigate unauthorised use of a telecommunications system and in the interests of national security. Many digital forensics professionals will find themselves making use of their provisions which overcome what would otherwise be an employee's reasonable expectation of privacy.

In the UK the extent of law enforcement powers include the Police and Criminal Evidence Act 1984 , which covers the physical seizure and subsequent examination of computers, the Investigatory Powers Act 2016, which deals with interception of voice and data traffic, access to and retention of communications data (who spoke to whom, when, for how long and from what location) and equipment interference officially authorised hacking. The Regulation of Investigatory Powers Act 2000 deals with covert human sources and offences for failing to provide access to encrypted information. The UKs intelligence agencies, MI5, MI6 and GCHQ are governed by the Intelligence Services Act, 1994 as well as the Investigatory Powers Act 2016. Cyber firefighters need a clear view of what they can and can't do.

C. Technical and Expert Evidence

The issue of how evidence is to be presented arises as a digital investigation proceeds towards a potential trial. Often that will be via a digital forensics practitioner. Most witnesses before a court simply testify as to what they have seen and done. They do not provide any opinion or commentary. Some forensic practitioners will do no more than report that they were tasked to carry out a particular series of tests and to report on the outcome. In digital forensics this might be the technical measures necessary to make an accurate and complete copy of the data on a digital device; it might also include searching across that device looking for particular keywords and then producing documents which contain them. But more often, the practitioner is asked to provide background explanations of how particular types of digital technology work and to make interpretations of the actions carried out by the user of that device for example carrying out a series of searches via a web browser, producing a chronology of events, or a sequence of emails from which conclusions might be drawn. At that point the practitioner becomes an expert witness. Courts welcome the presence of individuals who can assist them on matters which ordinary people may know little of but they are also anxious to ensure that the expertise is real, reliable and that someone who is expert in one field does not offer opinion in another. Courts are also anxious that expert evidence has a strong scientific basis. In some countries there is a requirement that courts experts are both accredited and registered ; in others such as the United Kingdom the emphasis is on the format and detail of an expert report and with a judge determining an individual's expertise . Assessment of whether a procedure is scientific may follow the US Daubert rules or some variant. And forensics course also need to take note of the debates about moves to accredit procedures and laboratories according to an international standard such as ISO 17025.

Increasingly some courts are requiring meetings between opposing experts to identify areas of agreement and disagreement. The aim is to shorten a trial. These can be pre-trial, as in the UK or via hot tubbing where the experts argue and can be cross-examined concurrently in front of the court as in Australia. Such meetings can make considerable demands on the professionalism of experts, particularly in the preparation of joint reports. It is essential that any digital forensics degree ensures that candidates understand their roles and duties as expert witnesses.

D. Disclosure/ Discovery

Disclosure - also referred to as *discovery* in the United States and elsewhere - is the requirement in a criminal trial that an accused has access not only to the evidence adduced against him/her but is also made aware of any other material gathered during an investigation which might either undermine the prosecution's case or support a defence case. In civil litigation disclosure is the mutual obligation of the parties to make the other side aware of the existence of documents which might undermine their case or support a defence. The effect on experts can be profound as they may need to show all the work that they have carried out during the course of an *instruction* to carry out a technical investigation and to prepare a report for use in court. Volumes of potential digital evidence, the product of how digital devices are used, have created an important sub- industry for digital forensic practitioners. In the UK there is a formal questionnaire which the courts expect to be used and a similar one operates in the US. In addition digital forensic skills and tools are being used to carry out effective searches for material which should be disclosed. Particularly in civil litigation where there may be vast archives of documents and emails; resort is being made to machine learning to expedite the searches. The parties agree to identify typical documents which qualify for disclosure, the machine learning program develops a set of rules to define the qualities of those documents and the rules are then applied to the archives that both parties hold. This is sometimes called Technology Aided Review or predictive coding. There is significant strand of

Year 1	Semester 3	Masters Project (60 credits)		
	Semester 2	Electronic Discovery and Data Analytics (20 credits)	Technical and Expert Evidence (20 credits)	Research Methods & Project Management (20 credits)
	Semester 1	Information Security Management (20 credits)	Digital Forensics (20 credits)	Advanced Ethical Hacking (20 credits)

Fig. 3. MSc Digital Forensics (Full Time)

Year 2	Semester 3		Masters Project [60 credits]
	Semester 2	Technical and Expert Evidence (20 credits)	
	Semester 1	Advanced Ethical Hacking (20 credits)	
Year 1	Semester 2	Research Methods & Project Management (20 credits)	Electronic Discovery and Data Analytics (20 credits)
	Semester 1	Information Security Management (20 credits)	Digital Forensics (20 credits)

Fig. 4. MSc Digital Forensics (Part Time)

research into the effectiveness of various methods.

It will be seen that in each of these three instances of IT law the digital forensics practitioner / cyber firefighter needs to embed into his/her everyday procedures in anticipation that their activities may be questioned as illegal or inadmissible, that they lack the necessary expertise or have failed to use proper scientific processes, or that they have not adequately recorded their activities so that they can be disclosed. The use of technology aided review is an important commercial development for litigation as well as a significant area for future research. For all of these reasons any digital forensics course needs fully to address legal issues both conceptually and as the implications for everyday practice. As with any attempt to teach law to non-lawyers it is important for lecturers to be able to produce examples and anecdotes at each stage and indeed, if possible, to invite students to ask questions and test scenarios of application.

E. Quality evaluation

We have used several evaluation methodologies to validate our MSc Cyber Security course before actually running it. We are going to use our experience of course design evaluation for the design of new MSc Digital Forensics curriculum. However, NCSC (a part of GCHQ) certification requirements for an MSc in Digital Forensics [5] will remain the predominant factor in the quality evaluation of this programme to ensure that we meet the quality requirements of pedagogic course of higher educational institutions as well as of specialised domain - i.e. Digital Forensics.

We also consider impact on student learning experience such as interactivity, engagement, higher employability, better student satisfaction rate, etc. We had held alumni workshops and consulted our existing students about these transformation together with running pilot sessions to identify gaps and discuss their fixes.

We have also solicited opinion of our industrial partners who are the potential employers of our students and therefore have greater interest in the development of our new curriculum.

V. Discussions

A number of recent high profile digital investigation cases have highlighted the need of additional set of skills and technological support for the Digital Forensic analysts to cope with the pressure of solving such unprecedented cases in the quickest possible timeframe. The major challenges are:

1) Enormous size of digital evidences being investigated nowadays (such as Panama Papers [6]) require better knowledge of Electronic Discovery (e-Discovery) [7] techniques and tools.
2) Advances in the area of high-speed networks [8] together with declining data subscription costs [9] have enabled a widespread use of contents streaming [10]. Investigations of contents-rich files consumes a lot of resources and processing time becomes quite lengthy [11]. It is therefore needed to give our students core knowledge of digital media processing to enable them to use rich media searching tools in their professional career.
3) A number of organisations (notably security and law enforcement) have a considerable backlog of their analysis tasks requiring efficient and innovative solutions such as:
   - Adding context in the plain-text searches (corpus linguistic [12])
   - Discovering patterns in multimedia searches (notably CCTV contents analysis)
   - Simplified algorithms for running efficient filtering/searches in gigantic datasets (big-data analytics)
   - Extracting device and network data (including roaming details) of mobile devices with variety of operating systems and applications including backend processing (mobile forensics)
   - Identification of operational anomalies in the contemporary smart environments consisting of interconnected devices (IoT/IoE), Industrial control systems (ICS), etc.
4) Understanding of core system instead of few common applications running on them.
   - For example, Skype uses Voice over IP (VoIP) protocol [13] for exchanging data packets. However, some of the recent cases have revealed the use of different VoIP software [14]. It is therefore imperative that our students understand how fundamental communication protocols e.g. VoIP work to be able to investigate a variety of apps using this protocol.
   - Another example is the essential knowledge of file systems and operating systems to enable our

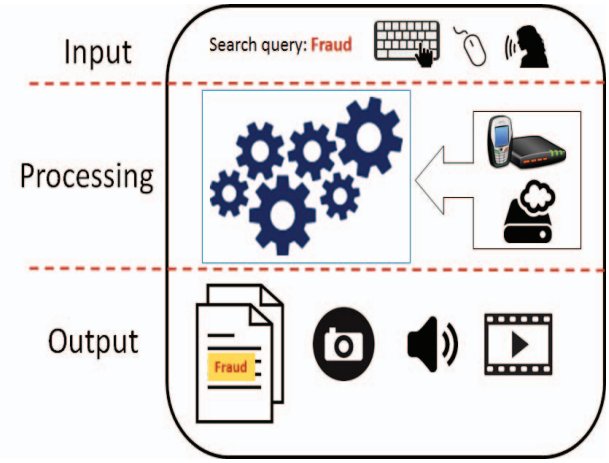

Fig. 5. Digital forensic analysis of comprehensive dataset

students to be able to analyse different artefacts such as data hidden in unallocated clusters that cannot be spotted by stenography detection tools.

- More importantly, they need to learn programming/scripting skills to tailor their investigation queries. As an example, following Adobe leak [15], an IT consultant of Vancouver was able to use a single terminal command grep to analyse thousands of email addresses to detect if any of his clients corporate or their customer data is leaked [16]. He managed to do it in a couple of hours instead of spending days or weeks thanks to his core knowledge of using shell commands.

5) Expert witness skills: Presenting the digital investigation results and being cross-examined is requiring more and more core knowledge of the digital forensic processes as well as the capacity to articulate the findings. Our students need these skills besides having appropriate appreciation of the legal and regulatory frameworks governing their digital forensic investigations.

These real-life investigation requirements should be reflected in a Digital Forensics curriculum as rapid pace of evolution in the area of cyber investigations and their scope should be at the centre of these courses and their delivery methods. The objective of this approach is to teach students the skills they need to meet the emerging challenges of scale, scope and complexity of cyberspace and their impact on analysing digital footprints. Students need a clear understanding of the core architecture of modern devices and systems. They need hands-on experience of the industry standard technologies for extracting data from these devices. Moreover, they need to develop a critical mind-set to be able to correlate findings to derive outcome of the investigations.

VI. Conclusions and Future Work

We have presented our work of developing Digital Forensic course on the basis of our successful design and delivery of Cyber Security course. This is a very hectic and demanding activity to ensure the satisfaction of a number of stakeholders and public sector regulators besides the businesses and potential employers of our students. The lessons learnt from this activity has proved extremely beneficial to help other courses and institutions to embrace change by ensuring continuous improvements in their educational offering.

We have a rich history of offering highly employable courses that have very well received by the employers. One way of maintaining these high standards is to regularly update our curriculum to reflect the emerging market needs and expectations of the businesses from the young workforce. We therefore involve all stakeholders in our curriculum development and transformation process. The overall learning outcomes are mapped to ensure that we have addressed quality standard bodies requirements as well as market needs.

Our future directions include adaptation of these courses for online delivery; and to offer to our overseas partners as part of our Trans-National Education (TNE). The adaptation is needed to have a better match with the technology constraints, global outreach, social and ethical implications.

Acknowledgment

The authors would like to thank University leadership, faculty management, course team members and academic services staff for their valuable support. We are also grateful to the staff of National Cyber Security Centre (a part of GCHQ) who provided us valuable guidance in better understanding of their certification requirements and processes.

References

[1] G. Dafoulas, D. Neilson, S. Hara, State of the Art in Computer Forensic Education-A Review of Computer Forensic Programmes in the UK, Europe and US, 2017 IEEE International Conference on New Trends in Computing Sciences (ICTCS) pp: 144-154
[2] IISP Skills Framework version 2.3 - https://www.iisp.org
[3] E. Yasinac, P. Marks, P. Sommer, Computer Forensics Education, IEEE Security and Privacy, Vol 1, Issue 4, July 2003
[4] UK Quality Assurance Agency for Higher Education - www.qaa.ac.uk
[5] NCSC degree certification - https://www.ncsc.gov.uk/information/ncsc-degree-certification-call-new-applicants-0
[6] M. Ingram, Behind the Panama Papers: How the Massive Document Leak Came to Be, Fortune Magazine, 04 April 2016
[7] D. Lawton, R. Stacey, G. Dodd, eDiscovery in digital forensic investigations, Home Office CAST Publication Number 32/14, ISBN 978-1-78246-465-5, 13 January 2015
[8] J. Wu, P. Fan, A survey on high mobility wireless communications: challenges, opportunities and solutions, IEEE Access Journal, vol. 4, pp. 450-476, 2016
[9] Ofcom (the communications regulator in the UK) report: Cost and value of communications services in the UK, 28 January 2014
[10] J. Mander, Trends 2016: Rise of Live Streaming, Global Web Index blog post, 07 January 2016
[11] A. Ho and S. Li (Editors), Handbook of Digital Forensics of Multimedia Data and Devices, Wiley-IEEE Press, ISBN: 978-1-118-64050-0
[12] S. Gries, What is Corpus Linguistics?, Language and Linguistics Compass 3, University of California, pp. 117, 2009
[13] M. Hillenbrand, J. Gotze, P. Muller, Voice over IP Considerations for a Next Generation Architecture, Proceedings of the 31th Euromico Conference on Software Engineering and Advanced Applications, 2005
[14] H. Mansoor, VoIP use by Safoora carnage suspects causes Sindh to invest in counter-strategy: Dawn Newspaper, 20 July 2015
[15] J. Dove, Adobe reports massive security breach, PC World Magazine online article, 03 October 2013
[16] R. Abbott, Free/Open Source Forensics Tools, Infosec Tools Issue of ISSA Journal, May 2015