Educating Digital Forensic Investigators at Newport

Stilianos Vidalis[1], Eric Llewellyn[2], Olga Angelopoulou[3]

[1, 2] Centre for Information Operations
University of Wales, Newport
stilianos.vidalis@newport.ac.uk
eric.llewellyn@newport.ac.uk

[3]Information Security Research Group
University of Glamorgan
oangelop@glam.ac.uk

Abstract

Digital forensics is a multi-disciplinary applied science governed by strict and rigorous rules and regulations. Individuals pursuing a career in this discipline are required to have an interdisciplinary background drawing elements of practical experience from fields as varied as sociology, psychology, forensic science, computing and the law. Despite the above, there is no professional body or QA benchmarks that specifically govern education in this science. The subject area has proved popular and where the profession has traditionally been limited to a select circle of individuals from specific industry sectors, it is now open to all. To meet this demand, many product vendors and Higher Education establishments have developed programmes ranging from short training courses to full undergraduate and postgraduate degree programmes. All these educational offerings promote the fact that individuals will be trained to an appropriate level, however without clear benchmark or regulatory guidance, students face the risk of being ill-equipped for the challenges presented in industry. The challenge faced by educators is to train individuals, many of whom have no prior theoretical or practical experience in the aforementioned fields, to become digital forensic investigators. This paper discusses the approach used at the University of Wales, Newport to overcome this challenge. It demonstrates how industry requirements have influenced and shaped the learning styles adopted by the teaching team in order to produce high calibre graduates that are ready to engage in a career in digital forensics.

1.0 “Pro-logos”

“Λόγος” (logos) is a Greek word that was originally used to mean “word”, “speech”, “account” or “reasoning” [1]. In the University of Wales, Newport we use “ρητορικός λόγος” (rhetorical logos) [2] and the other modes of persuasion as they were defined by Aristotle [3] in order to “develop” and educate tomorrow’s digital forensic investigators. “Πρό-λογος” (Pro-logos) [1] is what comes before the reasoning, so before we start reasoning we will try to “set the scene” by providing evidence and background information to our arguments that will follow in our “λόγος” [1]. We will start our journey of reasoning by setting some axioms and requirements, axioms that we will establish through the use of definitions and requirements that we will identify through the analysis of those definitions. We will then attempt to link those requirements to learning methods and programme learning outcomes.

The field of digital forensics has developed from forensic science and it is clearly important to gain an understanding of that discipline (requirement 1). Forensic science is used to give an insight to the chain of events that occurred during a crime. The Concise Oxford dictionary [4] defines the word forensic as “*relating to or denoting the application of scientific methods to the investigation of crime”*. The definition of forensic science also establishes the need to further understand what “crime” is (requirement 2).

According to Schweitzer [5] , digital forensics is “*the science of acquiring, retrieving, preserving, and presenting data that has been processed electronically and stored on computer media.”* Caloyannides [6] expands that it is “*the collection of techniques and tools used to find evidence in a computer.”* Palmer [7] defines digital forensics as: “*the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.”* Taken together, these definitions establish that there is a requirement to understand a digital crime scene (requirement 3) and be able to apply tools (requirement 4) and correctly follow processes (requirement 5) for retrieving, preserving and presenting electronic data.

Digital forensics encompasses all aspects of the investigation of computer related crime in dealing with a number of situations from industrial espionage to damage assessment. Clearly, expanding requirement 2, there is a specific need to understand what “computer related crime” is. Mohay *et al* [8] mention the first computer forensic practices back in the 1970s with mainframe computer systems. However, it was not until the 1980s that the need for computer forensics started to develop from a law enforcement perspective [8]. Despite the Internet revolution and the increasingly high profile of cyber crime, it is only in the last couple of years that terms like computer forensics and digital evidence have become widely known to the public along with an awareness of the expertise that is required by industry and the government [9].

Residual data on digital media can provide evidential information for a variety of different crimes. There has been an increasing body of on-going work examining the need for standardising the computer forensic investigation and valuable attempts for formalising the procedure have been published from both the law enforcement/industry and the academia (see [10], [11], [12], [13], [14], [15]). There are over one hundred [16] different models that appear in literature concerning digital forensics investigations attempting to aid the analysis of computer crime incidents. There is a clear need for understanding these models (links to requirement 4). A digital investigation relies on both system and human aspects (see [13], and therefore there is a need for analysing and evaluating the criminal mindset through cyber-criminal profiling (requirement 6).

From the discussions above it can be seen that digital forensics is the use of science and technology to investigate and establish facts in criminal or civil courts of law where digital forensic investigators apply science to the law. The need to understand legislation and legal proceedings is paramount (requirement 7). Forensic Investigators search and examine traces for establishing or excluding an association between someone suspected of committing a crime and the scene of the crime or victim. Their aim is to reconstruct the crime scene and provide evidence to reconstruct the crime [11]. They can act on behalf of either side in a case be it prosecution of defence solicitors for criminal matters or plaintiff or defendant in civil matters [17]. A Forensic Investigator will present his findings and opinions in written form either as formal statements of evidence or reports. The need to produce accurate expert witness reports is clearly vital in the role (requirement 8). In many cases a Forensic Investigator is required to attend court to present their evidence in person. Given the nature of the court room environment the ability to formally present often technical information in front of a large, and sometimes hostile, audience is vital (requirement 9).

To summarise, the digital forensic investigator has to have a skill-set that includes:

1. Understanding of the forensic science principles
2. Understanding of the different types of computer crimes
3. Understanding of managing a digital crime scene
4. Ability to use with competency digital forensic analysis tools
5. Ability to follow strict policies and procedures with meticulous record keeping
6. Reasonably good understanding of people.
7. Knowledge of evidence law and legal procedures.
8. Ability to write reports on technical issues in a non-technical manner
9. Ability to address large audiences in a formal manner and affect their decision making process.

The Division of Computing at the University of Wales, Newport began offering an honours degree for Forensic Computing in 2006. The program was initially based on the generic computing program with computing specific modules being replaced, in small numbers, by those with a digital forensics bias. The generic BCS computing guidelines [18] were used as learning benchmarks to guide the development of the programme which still focussed heavily on software design and development. The appointment of a Forensic Computing specialist saw the course refocused into a much more targeted programme with its sights clearly set on digital forensic investigations. The current programme team [19] has been proactive in approaching various product providers, Law Enforcement Agencies and the government to establish their training requirements, procedures, codes of conduct and their overall requirements for a potential employee. Having been continuously reviewed over three academic cycles the programme was completely redesigned and has become an almost autonomous cluster from the mainstream undergraduate computing programmes uniquely bringing the students in contact with the sciences of forensics, computing, law and behavioural psychology. Through Strategic Insight Programmes a number of other industrial partners have been consulted to gain vital information about their employment requirements, which have been directly integrated in the programme structure through individual module learning outcomes.

Naturally the ACPO guidelines [15] were used as benchmarks but as it will be evidenced by our "λόγος" [1], the programme at Newport enhances rather than regurgitates them. The programme makes use of a specialised laboratory infrastructure and, in comparison with mainstream computing, employs a diverse range of learning methods and techniques. The focus at Newport is to assist students in developing a high level of professionalism, based on the BCS code of conduct [20], and facilitate an environment that gets them to think outside of the box whilst still following specific processes for the transition from initial problem identification through to the recommendation, justification and presentation of a solution and its implementation.

2.0 "Paidagogia" for Digital Forensic Investigators

For justifying our programme delivery method the authors will use Plato's allegory of the cave [21]. Plato suggests that there are two different forms of vision, a "mind's eye" and a "bodily eye." The "bodily eye" is a metaphor for the senses. While inside the cave, the prisoners function only with this eye. In our situation, the "prisoners" is a metaphor for the full time students that "operate" in the protected academic environment of their University, which is the cave. The "mind's eye" is a higher level of thinking, and is mobilized only when the prisoner (the student) is released into the outside world and in our case when the student graduates and gets a full time job. Plato suggests that this eye does not exist within the cave; it only exists in the real, perfect world, hence the students cannot really mobilize their higher level of thinking in the traditional academic environment as they are force fed knowledge and skills by their tutors. Based in Plato, the "bodily eye" relies on sensory perceptions about the world in order to determine what reality is. Inside the cave, the prisoners believe that the shadows they see on the wall are actual reality, and in our case, students believe that the "traditional" academic exercises, academic reports and exams are the reality. Their "bodily eye" tells them that that world is real because their senses perceive so. Plato though suggests that the senses do not perceive the actual truth. The "mind's eye" is not active inside the cave because the prisoners are imprisoned in this distorted world, which they believe is reality. When one prisoner is pulled out of the cave and into the light, it is this sudden freedom that starts the gradual process of enlightenment. This sudden freedom opens the "mind's eye". In our case, when students graduate and are forced to act in the "real" corporate environment, combining their knowledge in solving real life problems, that's when the students can truly learn, develop and use their higher level of thinking.

In the previous section it was mentioned that the programme team is using "ρητορικός λόγος" (rhetorical logos) and the other two modes of persuasion for the "παιδαγωγία" (paidagogia) of the students. Paidagogia [1] is derived from the Greek word "παιδαγωγός" (paidagogos) which in ancient Greece it had the meaning of a boy-leader; a servant whose office was to take the children to school, a tutor. So, the tutors at Newport use "λόγος" (logos), "πάθος" (pathos) and "ήθος" (ethos) for the "παιδαγωγία". Logos is argument from reason and in Newport we look at the current investigative practice, we reverse engineer it, we identify and understand the reasons behind it and we reverse engineer those through arguments. Pathos is persuasion by means of emotional appeal, which means putting the hearer is a certain frame of mind, and in Newport we run a continuous simulation for the students from the moment they will enrol until the moment they will graduate, hence forcing the students into a certain mindset. We will discuss this at a later section. Ethos is persuasion through convincing listeners for one's character, and in Newport tutors lead by example and follow an entrepreneurial teaching method. This again will be explained at a later section.

Plato [22] reasoned that play is the best pedagogical mean in the education of a just citizenry and the cultivation of philosophical leaders who can apply their knowledge and experience to establishing a just city (*polis*) [23].

In Newport we use logos, pathos and ethos in order to "play" a simulation with our students and open up their "mind's eye" that will allow them to understand, think and deliver "outside of the box".

The "play" that we run at the University of Wales, Newport simulates the operations of a commercial digital forensics laboratory. We have developed the appropriate facilities including the hardware and software infrastructure that allows individuals to perform accurate and complete analysis of digital media that conform to UK legislation regarding admissibility of evidence [17]. The laboratory is a controlled access environment governed by strict usage policies and a code of conduct which is inspired by the BCS code of conduct [20]. This has been received very well from the students and as the laboratory usage data indicate the lab is being used by the students at more than 72% capacity every weekday between 09:00 and 17:00 during term time. The pinnacle of the student activities are the mock trials whereby the students report the findings of their investigations to a magistrate and are being cross examined by the Police. The elements of those activities include:

- Cross-validation of findings
- Proper evidence handling (MD5, SHA-1)
- Completeness of investigation
- Managements of archives
- Technical competency
- Explicit definition and justification of the process
- Legal compliance

3.0 Educating Digital Forensic Investigators at Newport

Best practice on learning and teaching from other Schools of the University of Wales, Newport and conclusions from primary data that have been gathered since 2006 from other successful programs in the NBS have been put together in order to form the learning and teaching strategy that is being followed for the delivery of this innovative award.

Firstly, having the digital forensics lab and running the simulation as it was explained in the previous section has made the students to come in when they don't need to. It has given them an exclusive club mentality and fostered a team spirit and a sense of belonging which is important and is discussed more extensively further down. The students enjoy their participation on events such as the annual E-Crime Wales Summit [24], specialised BCS events that include lectures and workshops and also engagement with Law Enforcement personnel through the various projects that the CIO is managing. Furthermore, students are being trained by external consultants on expert witness report writing and courtroom skills and they have the opportunity to achieve industry recognised training qualifications in the usage of digital forensic toolkits and networking.

For students to learn effectively and in depth they need to feel themselves as being valued and as belonging. It is only then when they are likely to be able to engage with the business of learning. The face to face teaching needs to be experience-based, problem oriented and learner-centred to enable students to understand and appreciate the inter-disciplinary nature of the award, and be able to link the theories with the real problems of the field.

Problem-based learning (PB)
Students working in small groups examining service user-centred scenarios or case studies that are driven by the needs/problems of the industrial partners of the CIO. The idea is that students work cooperatively in order to achieve both subject learning outcomes and transferable teamwork skills. This is addressed in the following modules: Professional Skills, Digital Evidence, Project Management, Computer Forensics Investigation, Network Security, and Cyber-Criminology.

Simulation-based learning (SB)
Students role-play with other students, guest lecturers and practitioners from the industry. Simulation provides a relatively safe context in which students are able to practice skills and receive feedback in a way that would not be possible in a real environment. The pinnacle of this method of learning is the mock trials in the final year of the degree where students present their investigation findings to a magistrate and they are cross-examined by the Police. Students receive appropriate training from external consultants on top of the activities with the programme team, in order to prepare for this event. This is addressed in the following modules: Professional Skills, Project Management, Digital Evidence and Computer Forensic Investigations.

Exchange-based learning (EB)
This approach emphasises the students exchanging their views and experiences and learning from each other in doing so. The course attracts many professional, experienced students and the tutors utilise their expertise in order to enhance the learning experience and provide a holistic view to the issues that are addressed through the subject learning outcomes. This is also addressed in the guest lectures that are provided during the semesters by practitioners from Law Enforcement Agencies and private organisations.

Reflective learning (RL)
Reflective practitioner theory emphasises relations between knowledge and experience and suggests that individuals reflect in an attempt to link theory to practice. Students are encouraged to reflect on their activities and processes of working together through team contracts and individual reflection reports that they have to prepare and submit for their formal assessments. This is truly when learning happens and when students manage to use their “mind eye” effectively, referring to Plato’s allegory of the Cave.

The important points that we are trying to address through the above learning modes are that learners:

1. Need to understand the relevance of what they are learning and how it relates to and has relevance for their future employment.
2. Prefer to take responsibility for their decisions and actions and value the ability to self-direct their learning.

3. In many cases have accumulated a great volume of experience, which enhances their learning and necessitates individualisation of learning strategies.
4. Relate better to things that they can equate with real-life problems.
5. Have a task-centred orientation to learning and like to feel free to focus on the task or problem.

We achieve the first point by providing to the students on overview of the programme learning outcomes and how they link to the module learning outcomes during their induction, and also through the individual module implementation plans every semester. We achieve the second point by using group assessments, and simulating the formal assessments as small projects, hence allowing the project teams to self-manage their learning activities. We achieve the third point by having individual meetings between tutors and project teams. We achieve the fourth point by introducing to the students the practitioners that have provided the case studies to the programme team, and allowing them to give guest lectures to the students explaining about the real-life problems that they have to overcome on their daily professional life. Finally, we achieve the fifth point by providing a 3 year project plan to the students, during their induction, identifying the tasks that they will have to perform, and how these link to the programme learning outcomes. The following table illustrates the programme structure and the four learning modes that are being utilised in each module as well as linking them to the nine industry requirements that were identified in the first section. All the modules are 20 CAT points except the Final Year Project that is 40 CAT points.

MODULE (prerequisites)	Learning Modes				Requirements								
	PB	SB	EB	RL	1	2	3	4	5	6	7	8	9
Year 1													
Software Development	√												
Professional Skills		√	√	√					√	√		√	√
Maths for Computing	√												
Forensic Computing		√	√		√	√	√						
Computer Systems	√												
Network Fundamentals	√												
Year 2													
Digital Evidence (FC)	√	√	√	√	√	√	√	√				√	√
Project Management (PS)	√		√	√					√	√		√	√
E-Crime (FC)	√		√			√	√						
Network Technology (NF)	√												
Legislative & Ethical Issues	√					√					√	√	
Operating Systems (CS)	√	√											
Year 3													
Cyber-Criminology (L&EI)		√		√		√				√	√	√	
Computer Forensic Investigation (DE, L&EI)	√	√	√	√	√	√	√	√	√		√	√	√
Final Year Project	√											√	
Network Security (NT, SM)	√	√		√		√							
Cryptology (Maths)	√												

The specific programme learning outcomes are:

1. Evaluate, select and effectively utilise a range of modern programming languages;
2. Analyse, evaluate and test a range of network systems including hardware, software and communications protocols;
3. Work independently or as part of a team to present information verbally and in writing which is well researched and appropriate for presenting evidence in a Court of Law;
4. Identify, critically evaluate, and counteract the security threats to standalone and networked computer systems;
5. Select and implement appropriate data types using a range of modern programming languages;
6. Discuss and interpret the moral, ethical, political and legal implications of computer crime;
7. Create and implement appropriate cryptosystems and security countermeasures;
8. Evaluate the roles, functions and concepts of operating systems and to evaluate them in terms of efficiency, robustness and security;
9. Analyse and diagnose computer misuse and its perpetrators and uncover evidence of cyber crime;
10. Gather, capture and interpret data which can be transformed into information and used as evidence.

The above programme learning outcomes further satisfy the following general aims that complement the identified industry requirements:

- Demonstrate sound knowledge and understanding of the concepts, theories and disciplines which underpin Digital Forensics.
- Conduct research into Digital Forensic issues and gather and evaluate evidence and information from a range of sources.
- Demonstrate cognitive skills of critical thinking, analysis and synthesis; and demonstrate the ability to solve structured and unstructured subject specific problems in unpredictable contexts.
- Communicate both orally and in writing, effectively and appropriately, using a range of formats and media relevant to Digital Forensic careers.
- Demonstrate effective self management skills; and demonstrate the ability to learn and work autonomously and reflect through self appraisal in appreciation of the need for continuing professional development and lifelong learning.
- Demonstrate the subject specific and transferable skills discussed in previous sections, to meet the demands of employers including creativity, team working, numeracy and a strong understanding of the legal and ethical requirements of modern businesses.

The following table links programme learning outcomes to modules:

MODULE (prerequisites)	**Programme Learning Outcomes**									
	1	2	3	4	5	6	7	8	9	10
Year 1										
Software Development	√				√					
Professional Skills			√			√				
Maths for Computing							√			
Forensic Computing						√			√	√
Computer Systems	√	√						√		
Network Fundamentals		√								
Year 2										
Digital Evidence (FC)			√		√				√	√
Project Management (PS)			√			√				
E-Crime (FC)				√						
Network Technology (NF)		√								
Legislative & Ethical Issues						√				
Operating Systems (CS)	√	√						√		
Year 3										
Cyber-Criminology (L&EI)						√				
Computer Forensic Investigation (DE, L&EI)			√						√	√
Final Year Project	√	√	√	√	√	√	√	√	√	√
Network Security (NT, SM)		√		√					√	
Cryptology (Maths)							√			

In Year 1 students develop a rigorous approach to the acquisition of a broad knowledge base regarding forensic computing. They learn to employ a range of specialised skills. They determine solutions to a variety of unpredictable problems. They evaluate information, using it to plan and develop investigative strategies. Students operate in a range of varied and specific contexts involving creative and non-routine activities. They exercise appropriate judgement in planning, selecting and presenting information, methods and resources. They undertake self-directed and a limited amount of directed activity. They learn to operate within specific guidelines and functions. They learn to take responsibility for the nature and quantity of outputs. They learn to meet specified quality standards.

In Year 2 students generate ideas through the analysis of information and concepts at an abstract level. They learn to command wide ranging, specialised technical, creative and/or conceptual skills. They formulate appropriate responses to resolve well defined and abstract problems. Students utilise diagnostic and creative skills in a range of technical, professional or management functions. They learn to exercise appropriate judgement in planning, design, technical and/or supervisory functions related to products, services, operations or processes. Finally, they learn to accept responsibility and accountability within specified parameters for determining and achieving personal and/or group outcomes.

In Year 3 students critically review, consolidate and extend a systematic and coherent body of knowledge in the field of forensic computing. They utilise highly specialised technical or scholastic skills across this area of study. They learn to utilise research skills. They critically evaluate new information, concepts and evidence from a range of sources. During Year 3 students transfer and apply diagnostic and creative skills in a range of situations. They exercise appropriate judgement in a number of complex planning, design, technical and/or management functions related to products, services operations or processes, including resourcing. They accept accountability for determining and achieving personal and/or group outcomes.

4.0 “Epi-logos”

“Επίλογος” [1] or “επί του λόγου” is a Greek word that literally means: what you have to say over your “λόγος”. We argued that there are four learning modes applicable for the learning of higher education students, and that we use “ήθος”, “πάθος” and “λόγος” to organise and “play” activities employing them for the delivery of the module content. Students feel valued and since their induction week they develop a feeling of belonging. All of the activities are driven by the research activities of the Centre of Information Operations and the students can comprehend that and that their learning is driven by applied research. Furthermore, the students are being recognised for the work that they do by practitioners, which is only inspiring their dedication.

This has an immediate impact to the student satisfaction and the programme has been scoring very high to the evaluation questioners that are being given out every semester. Industrial partners have also commented on the academic excellence that we have managed to achieve over the past 3 years, and this had an immediate effect to the externally funded projects that were awarded to the Centre of Information Operations.

The programme team is ready to proceed to the next level and we are looking in participating in the development of a Welsh Centre of Excellence in digital forensics with the participation and collaboration of the other Welsh Universities, the Welsh Police Forces, the Welsh Assembly Government and a number of private organisations. We are already developing training courses targeting Law Enforcement Agencies that will be employing the discussed educational techniques for the delivery of the training content.

5.0 References

1. Kypros-NET_Inc. *Greek-English Dictionary*. [www] 1998 [cited 2010 20th June]; Available from: http://www.kypros.org/cgi-bin/lexicon, 20th June.
2. Rapp, C. *Aristotle's Rhetoric*. Stanford Encyclopedia pf Philosophy 2002 June 2010 [cited 2010 20th June]; 2002:[Available from: http://plato.stanford.edu/entries/aristotle-rhetoric/, 20th June.
3. Brili, E., et al. (2010) *Aristotle: the politician and the philoshopher*. 20th June 2010.
4. Sykes, J.B., *The Concise Oxford Dictionary*. 1981: Clarendon Press.
5. Schweitzer, D., *Incident Response: Computer Forensics Toolkit*. 2003, Indianapolis: Wiley Publishing Inc.
6. Caloyannides, M.A., *Computer Forensics and Privacy*. 2001: Artech House Inc.
7. Palmer, G.L., *A Road map for Digital Forensics Research*, in *1st Digital Forensics Research Workshop*. 2001.
8. Mohay, G., et al., *Computer and Intrusion Forensics*. Computer Security Series. 2003: Artech House Inc.
9. Sheetz, M., *Computer Forensics: an essential guide for accountants, lawyers and managers*. 2007, United States: John Willey & Sons.
10. Carrier, B.D. and E.H. Spafford, *Getting physical with the digital investigation process.* International Journal of Digital Evidence, 2003. **2**(2).
11. Casey, E., *Digital Evidence and Computer Crime: Forensics Science, Computers and the Internet*. 2nd ed. 2004, Amsterdam: Academic Press.
12. Reith, M., C. Carr, and G. Gunsch, *An Examination of Digital Forensic Models.* International Journal of Digital Evidence, 2002. **1**(3).
13. Beebe, N.L. and J.G. Clark, *A hierarchical, objectives-based framework for the digital investigation process.* Digital Investigation, 2005. **2**(2): p. 147-167.

14. U.S.Department_of_Justice (2008) *Electronic Crime Scene Investigation: A Guide for First Responders*. 03/09/2008.

15. ACPO, *Good Practice Guide for Computer-Based Electronic Evidence*, ACPO, Editor. 2007.

16. Ieong, R.S.C., *FORZA - Digital forensics investigation framework that incorporate legal issues.* Digital Investigation, 2006. **3**: p. 29-36.

17. Jackson, M. and S. Vidalis (2010) *Digital Evidence and Legal Proceedings*. BCS, 20th June 2010.

18. BCS (2010) *Guidelines on Course Accreditation*. 20th June 2010.

19. IORG. *Information Operations Research Group*. [www] 2010 [cited 2010 20th June]; Available from: iorg.newport.ac.uk20th June.

20. BCS (2010) *BCS Code of Conduct*. 20th June 2010.

21. Brians, P. *Plato: the allegory of the cave, from The Republic*. [www] 1998 [cited 2010 20th June]; Available from: http://www.wsu.edu:8080/~wldciv/world_civ_reader/world_civ_reader_1/plato.html, 20th June.

22. Kamerling, G. *Plato*. 2006 2006 [cited 2010 20th June]; Available from: http://www.philosophypages.com/ph/plat.htm, 20th June.

23. Brown, E. *Plato's Ethics and Politics in The Republic*. 2009 [cited 2010 20th June]; Available from: http://plato.stanford.edu/entries/plato-ethics-politics/, 20th June.

24. eCrime_Wales_Steering_Group. *E-Crime Wales Summit*. [www] 2010 [cited 2010 20th June]; Available from: http://www.ecrimewales.com/, 20th June.