An Advanced Educational Tool for Digital Forensic Engineering

http://dx.doi.org/10.3991/ijet.v11i03.5294

Primož Cigoj[1,2], Borka Jerman Blažič[2]
[1] Jožef Stefan International Postgraduate School, Ljubljana, Slovenia
[2] Jožef Stefan Institute, Ljubljana, Slovenia

***Abstract*—This paper presents a novel approach to education in the area of digital forensics based on a multiplatform cloud-computer infrastructure and an innovative computer based tool. The tool is installed and available through the cloud-based infrastructure of the Dynamic Forensic Education Alliance. Cloud computing provides an efficient mechanism for a wide range of services that offer real-life environments for teaching and training cybersecurity and digital forensics. The cloud-based infrastructure, the virtualized environment and the developed educational tool enable the construction of a dynamic e-learning environment making the training very close to reality and to real-life situations. The paper presents the Dynamic Forensic Digital tool named EduFors and describes the different levels of college and university education where the tool is introduced and used in the training of future investigators of cybercrime events.**

***Index Terms*—cloud computing, cyber forensic investigations, digital forensic, dynamic forensics training, education, forensic tool, training environment.**

I. INTRODUCTION

E-learning has now been around for more than 10 years. During this time, it has changed from being a radical idea, the effectiveness of which was yet to be proven, to something that is now widely regarded as mainstream in modern education. It is also considered as being the core of numerous business plans and services offered by many colleges and universities [1]. Currently, e-learning tends to take the form of online courses in a virtualized environment. These courses differ in terms of technology and content, ranging from the resources distributed by MIT's OpenCourseWare project [2] to the design of learning materials offered by colleges and universities from all around the world, frequently acting as basic units for the organization of curriculums. The dominant learning technology employed for the management of e-learning is a system that organizes, delivers the online courses, and then follows the achievement of the learning objectives; it is called the Learning Management System (LMS). This piece of software, which is usually part of the university's network infrastructure, has become almost ubiquitous in most of the known e-learning environments. There are also attempts and practices to introduce blended teaching enriched with virtual environments, but this is still not widely deployed [3][4]. Other recent technologies, such as cloud computing platforms, are not yet heavily exploited in the area of e-learning. This is especially the case for education in cyber security and in the training of students in digital forensic engineering, which is a field associated with the fight against cybercrime and cyber terrorism. These fields are very specific and require intelligent, adaptable approaches that respond to user requirements, coming mainly from officers and members of LEAs (law-enforcement agencies), or private investigators, prosecutors and other cybercrime combatants. Criminal justice education, to which the field of digital forensic engineering belongs, is still conducted in a very traditional manner, especially when it comes to capturing digital forensic evidence and its subsequent analysis. The training environment for computer forensics and the methods for fighting cybercrime in most traditional institutions are carried out mainly as a static type of training as due to tradition they closely follow the traditional approaches in the criminal justice curriculum. The practical exercises and the challenges presented to the students are usually refreshed slowly and are frequently not up-dated with the most recent technology applied in cyber space. The exercises that accompany the curriculum are mainly carried out in class studying classic examples. The practical work is focused on solving a task known as “find the flag”, and the flag to be found is always at the same location where the training takes place. In real-life situations, the digital investigators are faced with much more complex tasks, and usually they are forced to use a wide range of methods and technologies to solve the problem [5]. This is due to the nature of the network technology applications and the speed of technological changes in the area of cybercrime and cyber terrorism, which remains a challenge that is not always well addressed [6].

Cybercrime attacks and internet use by terrorists encompass broad areas of engineering techniques and technologies, including human-machine interactions within complex economic and socio-technical systems [7]. In this context the training infrastructures that have been created so far usually do not provide the expected support for understanding the wide range of different scenarios that happen in the real world within the digitally based, sophisticated services and systems. In cases when such support is provided, they are often difficult to setup correctly and require extensive technical support, expertise and knowledge [8]. Together with this, the exercises used in the training process are usually abstracted to match the pedagogy level of the implemented cybercrime curriculums and the automated assessment of the students' performance as the resultant feedback that is part of the post-training assignments.

This paper describes a novel approach to education and training in the area of digital forensic engineering. The training is based on the use of a dynamic tool developed within the E-Forensics Educational Community that acts within the D-FET project consortium (Digital Forensic Education and Training project) and the underlying infrastructure. The tool is installed and available through the cloud-based infrastructure set within the D-FET project [9]. It is well-known that cloud computing introduces an efficient mechanism for a wide range of services offering real-life environments that can be used in the area of cybersecurity and digital forensics, which so far was not exploited well enough in this direction. The cloud-based infrastructure enables the construction of on-dynamic e-learning systems and tools, making this training very close to reality and to real-life situations [10]. The D-FET project is funded in the context of the EU's ISEC program [11] and its main objective is the development of an innovative educational approach in the area of digital forensics.

The tool we developed creates an ever-changing environment that is similar to the real environment in the cybercrime attacks happening on the Internet, allowing the training assignments to be generated as instances with different levels of task difficulty and to be accommodated individually for each of the trainees.

The paper is organized as follows: the next section introduces the cloud-based infrastructure and the basic features of the EduFors tool. The next section describes the technical details of the tool and the educational approach applied during the training process. The collected experiences of the performed training and the received feedback are presented in the fourth section, which is followed by a brief discussion and concluding remarks.

II. THE D-FET CLOUD-COMPUTING TRAINING ENVIRONMENT

The D-FET project is a training environment consisting of a virtual cloud-based platform that enables sharing of courses among the participating institutions and the use of laboratory training material without any restriction regarding the location of the student. The training environment is built up from virtual machines that are generated in a number depending on the number of enrolled trainees, meaning that the number of virtual machines will match the need and the requirements of the training. The training environment is dynamic and follows the evolving nature of the analytical cybercrime methods and approaches, as well as the technology development of cyberspace. The D-FET training environment caters for a range of educational levels, enabling education for Information and Communications Technology (ICT) students and as well as for law-enforcement professionals. Currently, the cloud infrastructure is owned and shared by the higher level educational institutions of the participating countries (Slovenia, UK, Ireland, and Sweden).

Figure 1 outlines the generalised training infrastructure and the approach used in creating real-life-based instances of cybercrime attacks or fraud, where an instructor has the possibility to generate an active instance for the training challenge, such as one related to finding data associated with a criminal act on a PC or on a smartphone, both accessible via the Internet. These active instances are generally based on known criminal use cases, such as the inves-

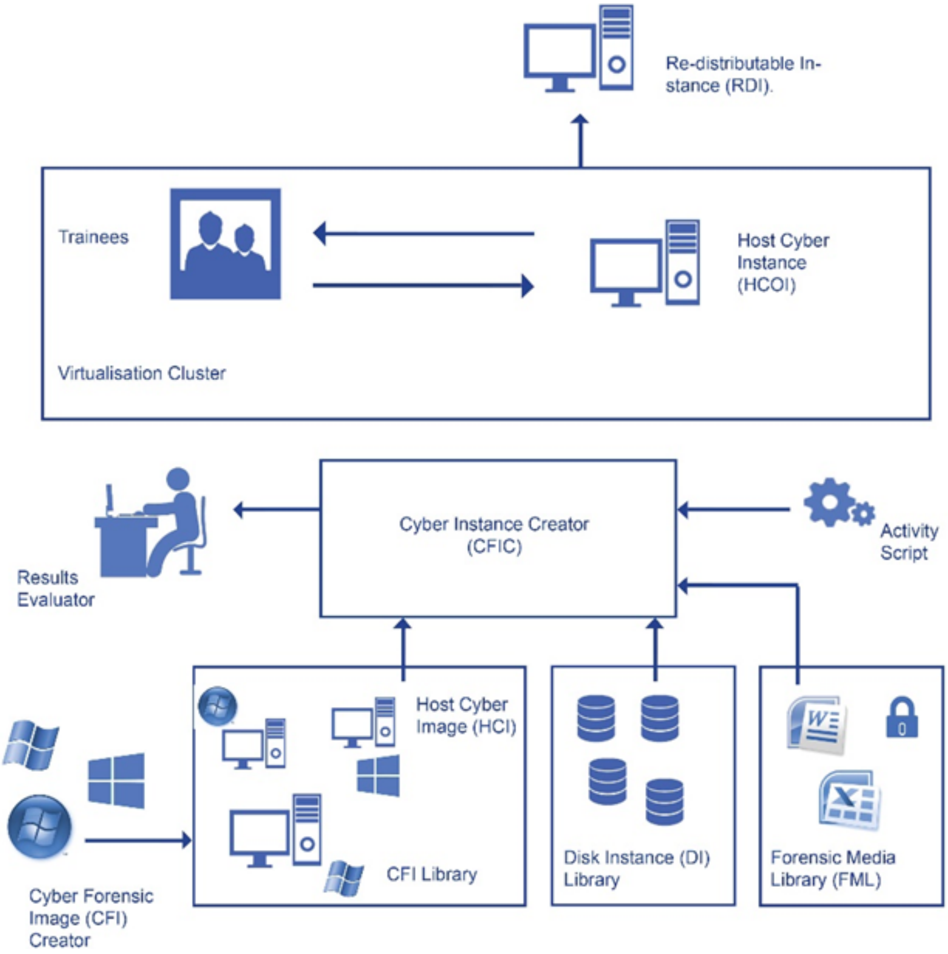

Re-distributable Instance (RDI).
Trainees
Host Cyber Instance (HCOI)
Virtualisation Cluster
Results Evaluator
Cyber Instance Creator (CFIC)
Activity Script
Host Cyber Image (HCI)
CFI Library
Disk Instance (DI) Library
Forensic Media Library (FML)
Cyber Forensic Image (CFI) Creator

Figure 1. The general training infrastructure

tigation of a computer for financial fraud, or a denial of service, where an investigation must create an evidence bag and handle the evidence correctly according to the legislative rules, making it credible and intelligible for use in a court. The cloud platform contains the incorporated educational tool known as EduFors, which is designed to provide several cyber forensic images, as instances originating from an attacked operating system or network server. Using this tool, multiple instances across the network are created and the challenge presented to the trainee is to collect the evidence from the criminal attack across a number of network-connected devices. The tool then adds the required disk instances for selected scenarios of different types of criminal acts and prepares them to be analysed by a known digital forensic tool, such as for example the X-Ways software package. These forensic analytical tools are stored in the Forensics Media Library built within the D-FET project and are triggered for use during the training process. Another key part of the process applied in education and training are the integrated metrics for the assessment of the trainee's performance. These metrics are related to the following:

- The time necessary to find the required evidence (which is limited in accordance with some predefined difficulty level);
- The investigation method used;
- The application of the correct parameters/indicators within the applied forensic tool.

Various levels of pedagogy/education are embedded in the system, allowing the educator to set different educational objectives that enable an assessment of the learning outcomes expected as results from the adopted training learning skills. The pedagogical levels and the educational approach follow the basic understandings of the learning theories, as defined in the Bloom learning taxonomy, split up into six different levels that proceed from the learning process [12]:

- Remember
- Understand
- Apply
- Analyse
- Evaluate
- Create

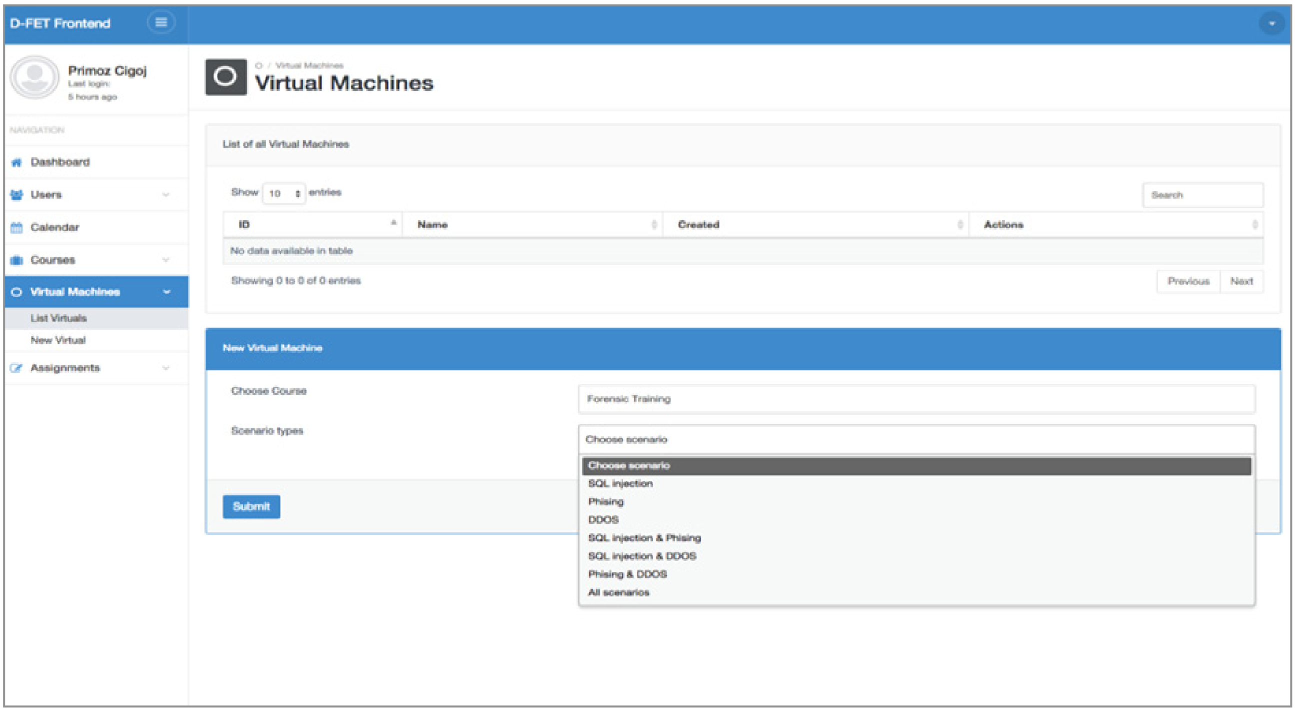
The parameters identifying the factual, conceptual, procedural and metacognitive learning outcomes are introduced in the assessment part of the educational tool. Here, we present only the main training process by providing an explanation of the properties of the EduFors tool.

III. THE EDUFORS TOOL

A. *Basic Architecture Description*

The tool is designed to generate instances based on known cybercrime scenarios and to present them to the trainee in a virtual environment created by the tool. The required levels of skills and understanding to solve the challenge are accommodated in such a way to reflect the different educational levels intended to be employed in training the different trainee groups.

The EduFors tool consists of two building blocks: the front end, which communicates (using an API – Application Interface), with the backend part. The latter is responsible for the generation of the instances representing different cybercrime situations. It also manages the training process. The front end allows the trainees to enrol in the system and to gain access to all the available courses for the selected level of education. The appointed administrator of education creates the paths to access the courses, gives assignments to trainees and manages the virtual machines generated in different platforms that are present in the cloud. This part of the system is also responsible for the presentation of the log files, the generation of the images of the attacked operating system and the injection of



List of all Virtual Machines

Show 10 entries

ID	Name	Created	Actions
No data available in table			

Showing 0 to 0 of 0 entries

New Virtual Machine

Choose Course: Forensic Training

Scenario types: Choose scenario

- Choose scenario
- SQL injection
- Phising
- DDOS
- SQL injection & Phising
- SQL injection & DDOS
- Phising & DDOS
- All scenarios

Figure 2. The EduFors forensic virtual machines

standardised templates for each of the crime scenarios selected for examination by the trainee. The tool manages the virtual machines on the remote cloud platforms. Representational State Transfer (REST) access is used (REST over the HTTP protocol) for communications with the remote terminal used by the trainee. The data are exchanged in the JSON format.

The registration of the trainee is possible by direct onsite registration or via a social network account (e.g. Facebook). Adding a new course to the system is fairly straightforward, as only the title and the description of the course must be entered, together with the duration of the course, accompanied by the course material. Once the trainees are registered and the courses saved in the system, the administrator starts the preparation of the virtual forensic machines. Six combinations of cybercrime scenarios are currently available in the EduFors tool, but there are plans to add more. Every time the administrator creates a new virtual machine for each of the existing scenarios, a different dynamic attack is applied to the machine. As illustration, Figure 2 shows the list of pre-created virtual machines and the available crime scenarios stored on the forensic disks, with the crime-attack data that are afterwards embedded in each template presented to the trainee. The dynamic template for each type of criminal attack and for each trainee are unique because of the different instances and the injected data prepared by the tool. The trainee has the impression of investigating on a real machine connected to a real IP network.

Each of the criminal attacks is presented to the trainee as a standard template, stored on the virtual machine together with the respective forensic disk. The templates presented to the trainee differ from the templates presented to another trainee in terms of the injected data and the required level of skills and knowledge that a particular cybercrime case requires for solving, meaning the production of relevant evidence and information about the attacker.

B. *Training Scenarios and Assignments*

Currently, the EduFors tool generates dynamic forensic templates for the three most frequent cybercrime scenarios: phishing, SQL-based data leakage and a distributed denial-of-service (DDOS) attack. However, in the next version of the tool other cybercrime scenarios will be added according to the definition in the ISO standard [13]. All of them briefly presented below.

Phishing. In this scenario, the client Adam discovers that his bank account has been compromised using a phishing method. The scenario is constructed with the use of two virtual machines (A and C) and a bank server. The attacker has obtained access to the server C by exploiting a weak password protection, as s/he has created a fake website imitating the client bank's server. By sending forged emails to Adam, and inviting him to access his bank, the attacker tricks him into believing that he is actually accessing his trusted bank website. That causes the client A to send personal information to the fake host residing on the attacker server C, and misleading him into believing that he was exchanging information with the bank (server B). The implementation of the phishing scenario and the data capture for forensic analyses require a website that retrieves and stores the entered credentials, the MySQL database for storing the retrieved credentials and various server log files. The log files contain the data of the random accesses to the phishing site by the victims and by the attacker. The instances and the template data are provided by a script written in PHP language. It uses two parameters – the test name and the test sequence number, for example, "phishing 1". The script then runs the attack scenario by picking up a random date for the time when the attack occurred. A list of template logs is then preloaded from the template folder, which is then used to generate the victim logs in the Apache OS and for the MySQL log files. This script is executed on a special virtual machine with access to the VMware platform from the cloud and the respective data storage. The template containing attacker relevant data is selected and the template placeholders are replaced with randomly selected data. These random data are consisting of the IP address, the date and the timing when the accesses happened. The IP address is unique to the whole log and is not repeated for any other victim logs. The populated template, based on these data, is then stored within the output file to be presented to the trainee. In each training day a random number of events can be generated and the range is between 6 and 24. To make the attacker's footprint slightly harder to be found by the trainee, additional data lines are added on the top of the log files (e.g. log data about previous events for several days up to 10). The same is done at the end of the log files (for 1 to 10 days). The days are generated incrementally and non-incrementally from the remainder of the generated log, so the resulting logs are listed in chronological order, looking very real and genuine. The generated data are stored in the local MySQL database (the attacker's IP address, the date and the hour of the attack and the type of scenario). A prepared, empty, virtual disk image is copied and mounted as a local file system using the libguestfs tool [14]. The prepared logs are then injected into the virtual disk image, the virtual machine template is cloned on the VMware server and the modified disk image is uploaded to the data storage. This approach allows for a new virtual machine to be prepared for inspection of the next forensic image by another trainee. The data prepared for inspection, along with the virtual-machine identification, are then returned as an output for the trainee in JSON format. The trainee receives a template of Adam's PC and the templates with data from the compromised server. In this scenario, the assignment given to the trainee consists of the following tasks:

- find the IP source address of the attacker,
- explain how the attacker has exploited the bank server,
- locate the directory where the fake website of the bank is hidden,
- explain how the attacker stored the required data for the phishing scenario,
- locate the other victims' IP address(es).

The answers to these assignments are then stored and checked for correctness, and an evaluation based on the percentage of correct answers is then provided.

Data leakage and SQL exploit. In this scenario, a website is the victim of an SQL injection attack. The attacker has used the web search bar to access the website's database. When the administrator of the attacked web server comes to the conclusion that the web data are compromised, he immediately contacts the police. The server is then disabled to prevent any further exploitation by the attackers and the data from the logs are brought to the trainee.

The crime scenario for the data leakage and SQL exploitation is provided by the same script as for the generation of the phishing scenario. The differences lay in the task generation and the use of different log templates and website structures. The websites in the cloud machines dedicated for training are modified in a manner to make them vulnerable to a SQL injection. The feature allows the attacker to run a multi-query MySQL statement, including the uploading of a binary file and saving it directly into a web-accessible folder. This attack is usually accomplished with an open-source tool known as SQLMap, which implements the SQL injection method and allows the execution of remote SQL statements. Several security features of the configured machine dedicated to training must be disabled as the most recent OS Ubuntu software versions contain patches that protect the OS from identified security vulnerabilities (usually known as SQL injection). Some of them are: prevention of writing MySQL data into the Apache's /var/www/html folder, and removal of the MySQL access to the group www-data, etc. The Ubuntu OS was also recently upgraded with other security features to prevent this type of attack e.g. denial of use of the multi-query MySQLi function, which allowed the execution of additional full SQL statements (as opposed to generally used, single-query, MySQLi functions that are not vulnerable to SQL injection attacks).

The file that generates the template data for this type of attack is also a PHP script in the form of a web file allowing simpler uploading of additional scripts. The scenario is based on the publicly accessible PHP shell and the script known as "cyb3r sh3ll". By exploiting these scripts, the attacker can retrieve various types of information from the server database. The template presented to the trainee for SQL injection attacks provides the specific filenames of the attack scripts and the SQL queries that they execute. As an addition to the MySQL log, the script also attaches the SQL injection query that has executed the attack. The assignments for this scenario given to the trainee are the following:

- Decide whether an SQL injection occurred on the particular identified server;
- Identify the IP source address of the attacker;
- Find which data were compromised;
- Fix the attacked website.

Distributed Denial-Of-Service (DDOS). A DDOS scenario is implemented in the same way but the log templates generated for training are different. This attack is implemented by simulating a small-scale DDOS attack initiated from several machines. Some of them are just normal computer-machine clients, and others are virtual.

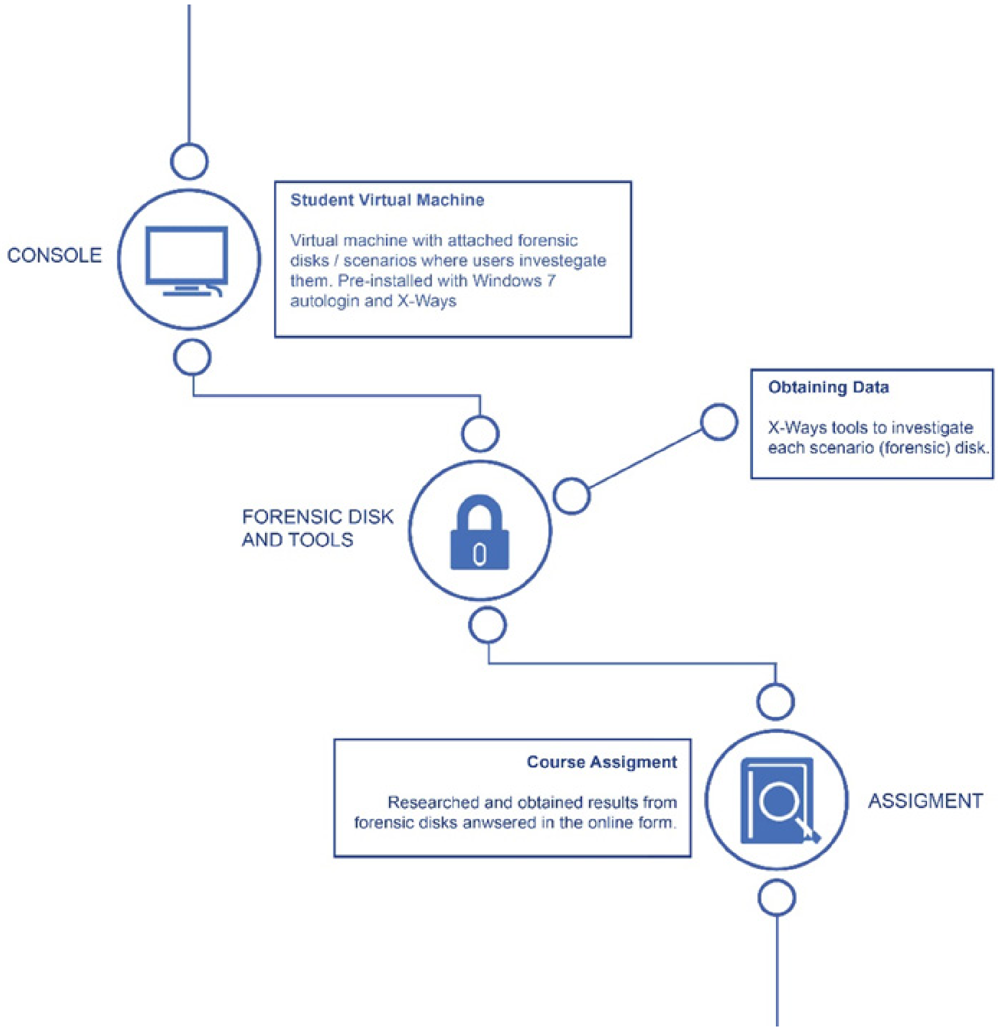

CONSOLE
Student Virtual Machine
Virtual machine with attached forensic disks / scenarios where users investegate them. Pre-installed with Windows 7 autologin and X-Ways
Obtaining Data
X-Ways tools to investigate each scenario (forensic) disk.
FORENSIC DISK AND TOOLS
Course Assigment
Researched and obtained results from forensic disks anwsered in the online form.
ASSIGMENT

Figure 3. EduFors process

The network traffic for the required evidences is captured on the victim's server. The script for this scenario picks a random date to indicate the date when the attack has occurred. A list of template logs is then preloaded from the template folder to the Apache server log files and presented to the trainee. The assignments given for this type of tasks are as follows:

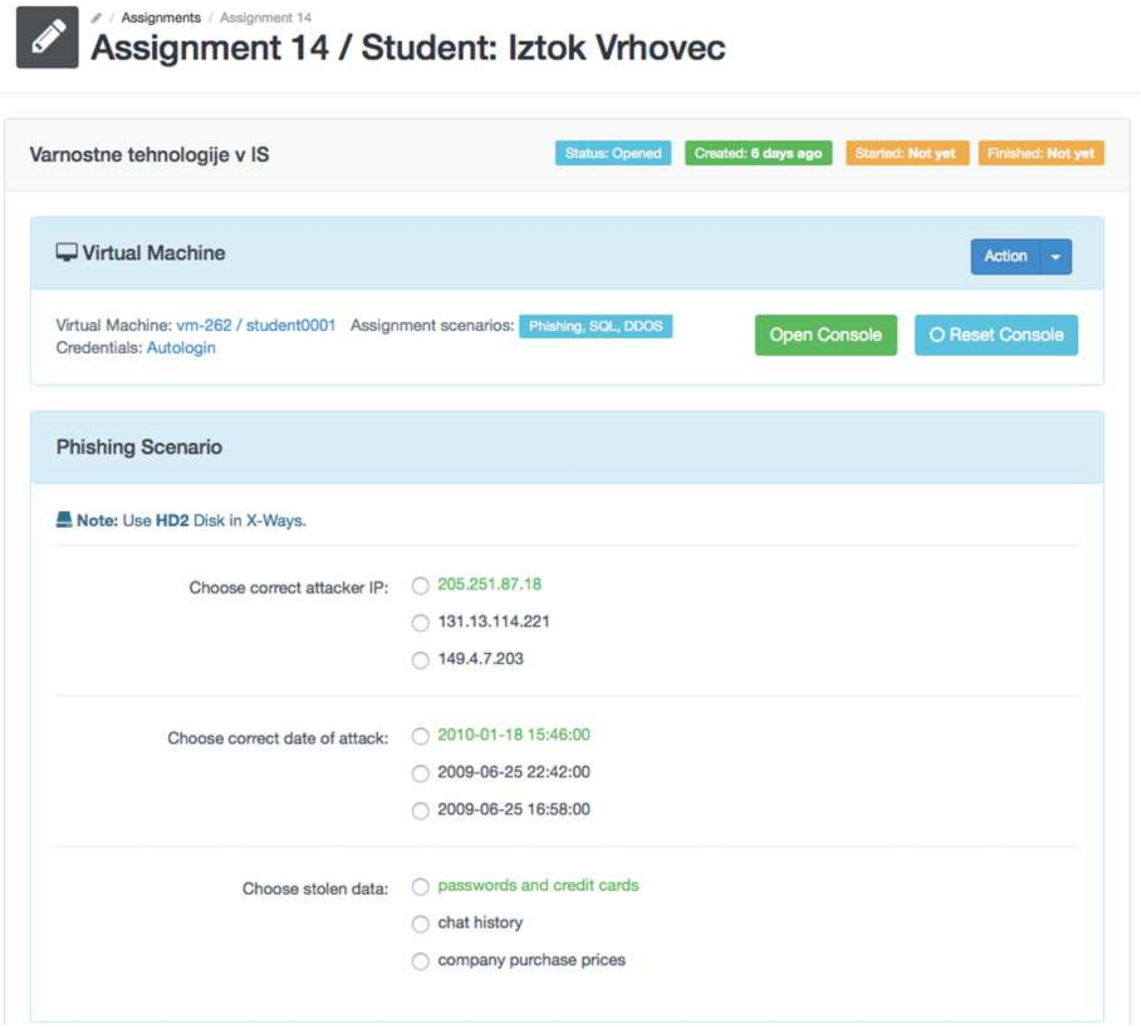
- Decide whether a DDOS attack has occurred;
- Identify the IP source address of the attacker(s);
- Find if a botnet network was involved in the attack;
- Assess the damage, taking into account the time for which the server was disabled;

An illustration of the processes run by the EduFors tool during the laboratory training is presented in Figure 3.

IV. EDUCATIONAL LEVELS AND LABORATORY TRAINING

There are two ways to obtain credit within the D-FET educational cloud-platform environment. The first uses the provided training material and the tasks set by different assignments, which guide the trainee through a set of learning outcomes when s/he has absorbed the knowledge from the theoretical part of the course and the required skills from the training part with the EduFors tool. This involves studying the theoretical background provided in the context of the selected course(s), the inspection of the virtual instances for cybercrime scenarios that are part of a particular training package and the solutions of the aligned training assignments required in a cybercrime investigation. The success of the training is evaluated with the defined learning metrics. The data required for the assessment are collected after the learning is completed, and the achieved transfer of knowledge is inspected by the training tool and the answers to the questions from the theoretical part. Before the start of the training the trainee is asked if s/he has understood the assignments and the assessment that will follows after the completion of the assignments. The collected feedback from the trainees' results is evaluated using the tool, and the results from the theoretical part are used in the final assessment of the educational outcomes.

With the D-FET platform the standard training element consists of 3 hours of laboratory practicing in a computer lab and a training session, which typically involves an online introduction to a particular lesson(s), followed by the interactive practical session with the EduFors tool that provides an itemized feedback. This feedback can be then used to calculate a credit that is added to a particular training package if the lecturer decides to do so.



Assignment 14 / Student: Iztok Vrhovec

Varnostne tehnologije v IS

Virtual Machine

Virtual Machine: vm-262 / student0001 Assignment scenarios: Phishing, SQL, DDOS
Credentials: Autologin

Phishing Scenario

Note: Use **HD2** Disk in X-Ways.

Choose correct attacker IP:
○ 205.251.87.18
○ 131.13.114.221
○ 149.4.7.203

Choose correct date of attack:
○ 2010-01-18 15:46:00
○ 2009-06-25 22:42:00
○ 2009-06-25 16:58:00

Choose stolen data:
○ passwords and credit cards
○ chat history
○ company purchase prices

Figure 4. Assignment for the phishing scenario

EduFors is currently used as the training part of courses which are part of a classic academic curriculum, e.g. the ICT MSc postgraduate level, with the respective academic credits. However, during the academic course the EduFors tool is available to enrolled students to practice, and the itemized feedback provided after the exercise is an information that helps the students to assess their progress in the learning process.

The D-FET partners offer academic credits for an MSc qualification, based on a pool of modules. The qualifications that can be achieved by the MSc students are the following:

- Post-graduate certificate, worth 30 ECTS;
- Post graduate diploma, worth 60 ECTS;
- Post graduate MSc, worth 90 ECTS, which must include a dissertation worth 30 ECTS credits.

This list of credits is included in the post-graduate academic programmes provided at the DFET project institutions, which are:

- MSc in Advanced Security and Digital Forensics (full-time, part-time and distance learning). Consists of six teaching modules and a dissertation, Edinburgh Napier University (ENU);
- MSc in Advanced Networking with Information Security (full-time, part-time and distance learning). Consists of six teaching modules and a dissertation (ENU, Institut Jozef Stefan, IJS);
- MSc in Cybercrime (work-based learning). Consists of three distance-learning modules, a work-based learning module, and a dissertation (ENU);
- MSc in Information Security, Stockholm University (SU).

Each package includes laboratory work composed of the assignments generated by the EduFors tool. The assignments are presented to the student as a choice of available scenarios prepared for a particular educational level and the associated laboratory training. The student selects a one-by-one scenario as a result, and finishes the training after the task assignments have been solved successfully (The EduFors example of an assignment is presented in Figure 4). After the student finishes the assignment tasks, the educator evaluates the parameters provided by EduFors such as the time spent and the correctness of the solved forensic problem(s) to generate the amount that will be added to the credits that are being collected for the particular course. EduFors collects the following data: the time slot between the opening of an assignment and its closing, and the time the student has used to accomplish the task or to answer the questions. If the time spent for solving the tasks is longer than the pre-allocated time for each task, the information is acknowledged and the tool ads negative point to the scores appointed for correct answers. The allocated time per assignment differs and depends on the difficulty level required for the task solving. If 50% of the answers submitted by the student are correct and the time is not exceeded, the tool gives a positive score. However, this percentage can be changed by the educator, depending on his/her requirements regarding the study level. For each participant in the training, e.g., the trainee, the educator and the administrator, the tool provides a different dashboard adapted to the different roles of the participants, for an easy monitoring of the progress.

V. ASSESSMENT

To assess the usefulness of the tool we followed the evaluation scheme for teaching and training difficult subjects proposed by El-Zein et al. in their study of blended teaching and learning computer programming [3]. Digital forensic is considered a difficult subject in the engineering education as it requires a good background of the computer OS and networking in addition to analytical skills and mind. The students enrolled on the Digital forensic subject are expected after successful accomplishment of the course to be able to develop good understanding of the forensic principles and methods. In addition, by the end of the course the students are expected also to acquire skills enabling them to perform simple forensic investigation by use of forensic software, such as X-Ways, and to decipher the output provided by the software.

After the first year of introduction of the new security course entitled Digital Forensic on the postgraduate program study of Internet technology it became obvious that interactive self-practice Lab exercises are necessary to carry out successful education. We have faced in that time with the problem of getting appropriate tool for individual training. The tool was not found and as a consequence the EduFors tool was developed. The situation of having two generation of students that enrolled the course allowed us a compare the success of the learning outcomes of the two generations of students: those who followed the classical curriculum with classical Lab exercises and the generation that had the possibility to be trained within the virtual environment provided over the D-FET infrastructure (now available as Cyber Academy [15]). In the first year the course was thought in a classic lecturing hall accompanied by practical exercise in the computer lab similar to the well-known teaching method [16] with installed forensic software. The next generation of students were trained with the EduFors tool. After the lessons presented at lecturing call the students were introduced with the basic information about the new virtual environment and the availability of the EduFors tool. Support and help was provided by assistants who were contacted via e-mail or during the open hours of the computer laboratory. Attendance and practicing in the Computer Lab equipped with access to the tool after the lessons was voluntary and open to all students who wanted to get extra training and support from the assistants or to get pro-active guidance. The main objection issued by the previous generation of students was about static appearance of the repeating examples provided and offered for examination to the forensic software. Another objection from the first generation was the lack of real cases and their resolving in close to reality where cybercrime act happens. The lack of this type of experience and understanding of some exam questions reflected in weak exam results as 22% of the students failed to pass the exam that consisted of theoretical questions (7 of them) and from (3 of them) practical cases of cybercrime attacks or other instance occurring malicious act on the network or on the computers.

The expressed objections and the law rate of exam success influenced the decision to design a learning tool that should be available on a cloud platform and will simulate as much as possible the occurrence of cybercrime attacks. In the first year the number of students was not so high (in year 2013, (13 students) and in 2014 23), the teaching was performed in small, conventional classroom but the training and practicing was performed in different computer environment. The development of the training tool was also stimulated by the new initiative of the three universities that collaborated in the D-FET project (Dynamic Digital Forensic Education and Training, funded by DG Imigration and Home. New infrastructure was set up with different courses from Cyber Security area with focus on Digital Forensic contents. The infrastructure enabled access from anywhere and use of the EduFors tool any time. Only proper student authentication was required.

The evaluation of the EduFors tool took place in the first semester in 2015 of the school year 2014/2015, more exactly in spring 2015. After the accomplishment of the course and after the exam were over the students were asked to express their opinion about the usability of the tool and the easiness it provides for training some of the steps of digital forensic investigation procedure. Comparison of the surveys carried about with the students from year 2013 about Digital Forensic course and the survey with the students from year 2014 has shown substantial improvements in the course assessment and in the exam results. Classical Licker scale was used with as follows:

- 1 – Strongly disagree
- 2 – Disagree
- 3 – Neither agree nor disagree
- 4 – Agree
- 5 – Strongly agree

The questions in the student questionnaire and the results from the first student generation are presented on Table I and the results obtained from second student generation are presented on Table II. The comparison of the data from Table I and Table II are shown in on Graph 1, where the data the significant difference of the exam success rate and evaluation improvement of the course is visible and convincing. The assessment score increased by 26% points.

It is obvious that the learning objectives of the course without training that with EduFors tool were much more difficult to be achieved. The first year students were capable to understand and interpret the products/files of the forensic software but they failed to identify the crime actor and the source of the cybercrime act which is a major goal of any digital forensic investigation. In the second year the student failures on the exam fall to only 12% compared to 22% of the first generation. So, despite the fact that this study has a limited timing of observation and

TABLE I. SURVEU OF THE RESULTS FOR 2013 – 13 ANSWERS

Question	Positive Answers	Negative Answers	% of all positive answers	Satisfaction
I was satisfied with the time provided for the exam.	7	3	54%	70%
The providing of instructions was satisfactory.	9	2	69%	82%
The forensic tool provided the information needed to solve the assignment goals.	1	8	8%	11%
It was easy to find the results with the provided forensic tool.	9	4	69%	69%
The exam evaluated various topics of different difficulties.	2	10	15%	16%
I find myself capable of solving tasks.	9	3	69%	75%
The hints were useful.	2	10	15%	16%
The tool was able to retain my attention throughout the test.	3	8	23%	27%
The tool guided me properly through the whole process of completing the exam.	1	11	7%	8%
I felt that I have entered the results correctly.	2	11	15%	15%
The environment to solve the assignment was easy to comprehend.	5	6	38%	45%
The course stimulated my interest in the topic.	7	4	53%	63%
I was satisfied with the lecture instructions and the way I achieved desired results.	7	3	53%	70%
I had a feeling that I will be able to generalize the knowledge and the skills acquired during the course.	6	3	46%	66%
I had sufficient knowledge to solve the assignment.	10	2	76%	83%

TABLE II. SURVEY OF THE RESULTS FOR 2014 – 23 ANSWERS

Question	Positive Answers	Negative Answers	% of all positive answers	Satisfaction
I was satisfied with the time provided for the exam.	17	4	74%	80%
The providing of instructions was satisfactory.	19	2	82%	90%
The forensic tools provided the information needed to solve the assignment goals.	16	5	69%	76%
It was easy to find the results with the provided forensic tool.	15	7	65%	68%
The exam evaluated various topics of different difficulties.	16	6	70%	72%
I find myself capable of solving tasks.	15	7	65%	68%
The hints were useful.	14	4	61%	78%
The tool was able to retain my attention throughout the test.	17	4	73%	81%
The tool guided me properly through the whole process of completing the exam.	15	5	65%	75%
I felt that I have correctly entered the results.	22	0	95%	100%
The environment to solve the assignment was easy to comprehend.	14	8	60%	63%
The course stimulated my interest in the topic.	13	8	56%	61%
I was satisfied with the lecture instructions and the way I achieved desired results.	14	3	60%	82%
I had a feeling that I will be able to generalize the knowledge and the skills acquired during the course?	15	7	65%	68%
I had sufficient knowledge to solve the assignment.	19	4	83%	83%

data collection, the conclusion still can be drawn that despite the increase of the level of difficulty of the exam questions (two practical question directly required digital forensic investigation report) that the used tool contributed to the better results.

To verify the approach a training course was offered to the public expert audience in January 2015 with a shorter program but accompanied with a training with EduFors. The feedback received enthusiastic and in general most of the answers gave very positive comments about the tool.

The experts that attended the seminar appreciated the EduFors capabilities that enable flexible training as each trainee advances in the learning by his own pace and is able to learn by invoking relevant additional explanations that accompany the lessons lectured in the classroom.

VI. CONCLUSION

Teaching digital forensics is a demanding area of education as it involves intensive, hands-on exercises that require students to follow potentially tedious procedures demanding a long and focused attention span. Due to these challenges, current forensics courses are often designed for advanced students who are capable of following a variety of demanding disciplines from the OS, IP networking and traffic monitoring, file system analysis, basic web applications or protocols. The knowledge of these disciplines is a prerequisite for students of digital forensics, so they are capable of absorbing advanced, abstract concepts used in discovering acts of cybercrime and frauds. The experiments used for training are usually tedious, static and are not frequently applied during the study. In this paper we have proposed an innovative idea to overcome some of the difficulties associated with education in digital forensics, based on a successful combination of visualization technologies and the dynamic generation instances in a real cloud-based computing environment. The current experiences point to the conclusion that this approach will be very effective in the teaching of digital forensics and in other advanced, computer-based fields that involve an understanding of abstract concepts and hands-on practice. Future work includes upgrading the EduFors tool with game elements that will contribute to the attractiveness of EduFors applications by serious game development in order this tool to trigger more attention from the learners and educators. We also plan to work on a further assessment and evaluation for measuring the effectiveness of the presented educational approach.

REFERENCES

[1] Downes, S.E.: Learning 2.0. The eLearn Magazine. (2005) http://www.elearnmag.org/subpage.cfm?section=articles&article=29-1, accessed 12th December 2014

[2] Massachusetts Institute of Technology: Open Course Ware project. http://ocw.mit.edu/index.htm, accessed 1st December 2014.

[3] El-ZEin, A., Langrish, T., & Balaam, N. I. G. E. L. (2009). Blended teaching and learning of computer programming skills in engineering curricula. Advances in Engineering Education, 1(3), 1-18.

[4] Dib, H. A. Z. A. R., Adamo-Villani, N., & Garver, S. T. E. P. H. E. N. (2013). An interactive virtual environment for learning differential leveling: Development and initial findings. Advances in Engineering Education.

[5] Hartel, P. H., Junger, M., & Wieringa, R. J. (2010). Cyber-crime science= crime science+ information security.

[6] Becker, R. A., Volinsky, C., & Wilks, A. R. (2010). Fraud detection in telecommunications: History and lessons learned. Technometrics, 52(1). http://dx.doi.org/10.1198/TECH.2009.08136

[7] Armitage, R., & Pease, K. (2008). Design and crime: Proofing electronic products and services against theft. European Journal on Criminal Policy and Research, 14(1), 1-9. http://dx.doi.org/10.1007/s10610-007-9043-6

[8] Henry, G., Baraniuk, R. G., & Kelty, C. (2003). The connexions project: Promoting open sharing of knowledge for education. Syllabus, Technology for Higher Education.

[9] D-FET project. http://www.d-fet.eu/project-overview/, accessed 5th December, 2014

[10] Laisheng, X., & Zhengxia, W. (2011, January). Cloud computing: a new business paradigm for E-learning. In Measuring Technology and Mechatronics Automation (ICMTMA), 2011 Third International Conference on (Vol. 1, pp. 716-719). IEEE.

[11] ISEC: Prevention and fight against crime. http://ec.europa.eu/dgs/home-affairs/financing/fundings/security-and-safeguarding-liberties/prevention-of-and-fight-against-crime/index_en.htm, accessed 18th December, 2014

[12] Anderson, L. W., Krathwohl, D. R., & Bloom, B. S. (2001). A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives. Allyn & Bacon.

[13] ISO, 2012. ISO 27037:2012 Information technology — security techniques — guidelines for identification, collection, acquisition, and preservation of digital evidence accessed 2nd Match, 2015

[14] Diagnostics for libguestfs. http://libguestfs.org/libguestfs-test-tool.1.html accessed 5th December, 2014

[15] The Cyber Academy. http://thecyberacademy.org accessed 10th March, 2015

[16] Hodge, B. K., & Steele, W. G. (2002). A survey of computational paradigms in undergraduate mechanical engineering education. Journal of Engineering Education, 91(4), 415-417. http://dx.doi.org/10.1002/j.2168-9830.2002.tb00726.x

AUTHORS

Primož Cigoj earned his master's degree at the Jožef Stefan International Postgraduate School. Prior to that, he studied computer science at the University of Ljubljana, Slovenia. Currently, he is a researcher and developer in information security at the Laboratory for Open Systems and Networks, Jožef Stefan Institute, Jamova cesta 39, 1000 Ljubljana, Slovenia. His research interests include cloud-computing server-side and client-side approaches to security in cloud computing. For the past year he has been focusing on the concept of Single Sign-On (SSO) implementation across open source and commercial cloud platforms. He is actively contributing to the KC CLASS (Cloud Assisted Services Competence Center) research. (e-mail: primoz@e5.ijs.si).

Borka Jerman Blažič is a full professor at the University of Ljubljana, Department of Economics, and is heading the Laboratory for Open Systems and Networks at Jožef Stefan Institute, Jamova cesta 39, 1000 Ljubljana, Slovenia. Under her leadership the laboratory has been involved for more than 20 years in European Union Framework Program projects in the area of ICT and related fields.

As full professor at the University of Ljubljana she is teaching undergraduate courses in "Electronic Communications" and "Information Security", and postgraduate courses in "Telecommunication Services and Technologies", "Legal Aspects and Standards in ICT" and "E-commerce". She is teaching "ICT Security in E-commerce" at the Postgraduate School of Criminal Justice, University of Maribor, and at the International Postgraduate School, Jožef Stefan. She spent her postdoctoral study period at Iowa State University, Ames, USA, and has worked as a project-development officer for TERENA – The European Association of Academic and Research Networks. (e-mail: borka@e5.ijs.si).

Submitted 18 November 2015. Published as resubmitted by the authors 25 February 2016.