*International Journal of Engineering Education* Vol. 30, No. 4, pp. 964–976, 2014
Printed in Great Britain

0949-149X/91 $3.00+0.00


# Ontology Based Model of Digital Forensic Virtual Lab and Curriculum Design*

IGOR FRANC
Faculty of Informatics and Computing, Singidunum University Danijelova 32 Belgrade, Serbia. E-mail: ifranc@singidunum.ac.rs

IVAN STANKOVIC
Business School of Applied Studies—Blace, Kralja Petra I 70, 18420 Blace, Serbia. E-mail: istankovic@singidunum.ac.rs

IRINA BRANOVIC
Department of Informatics and Computing, Singidunum University, Danijelova 32 Belgrade, Serbia. E-mail: ibranovic@ieee.org

RANKO POPOVIC
Faculty of Informatics and Computing, Singidunum University, Danijelova 32 Belgrade, Serbia. E-mail: rpopovic@etf.rs

Digital forensics (DF) is a discipline that uses investigative methods to find digital evidence and prepare it for legal proceedings in computer crime cases. Since this is a relatively new teaching subject in higher education institutions, syllabi and curricula are not yet standardized. In this paper we present an ontological approach to DF curriculum design, and discuss its implementation in a virtual digital forensic laboratory. The virtual educational environment is designed for the generic study of digital forensics, and is based on ontology and a composite-component approach. Basic components of our virtual DF are objects to be related, put into new compositions and placed in a library; relationships between all of the components are defined in ontology. Based on gathered experience, we designed and described DF curricula for undergraduate, graduate and Ph.D. studies that are tailored to our needs, but at the same time can be used as the starting point for introducing digital forensics courses at universities.

**Keywords:** digital forensics; ontology; curriculum design; 3D model; component-composite model; education

## 1. Introduction

Over the last few years, information technology has transformed the way in which organizations operate, making them vulnerable to hackers. Thus, they must rely on professionals to protect their computing systems. Computer forensics has been developed in response to computer crime. It refers to processes in which professionals use investigative methods to find digital evidence and prepare it for legal proceedings. It concerns the application of computer investigation and analysis techniques to solve a case and provide evidence to support it. In order to recover information from encrypted files or destroyed hardware, investigators often use specific applications and software programs to examine or extract specific types of data from files and folders. There are many tools available, such as Encase [1], FTK [2], SIFT [3], DEFT [4] and Helix [5]. Most of these tools require a knowledgeable expert to ensure that meaningful and relevant evidence is located and collected, not corrupted or compromised during the acquisition process. Forensics experts must also document their findings in a structured way, learn about different legal processes involved in an investigation and make sure that the level of integrity of evidence is always high.

The term 'Golden Age DF' refers to the period 1999–2007, when a rapid development of Digital Forensics (DF) took place. This period is characterized by the following.

- Proliferation of Microsoft Windows OS (mostly Win XP).
- A relatively small number of file types that are relevant to a DF investigation (MS Office, jpeg, avi, wmv).
- Investigation concentrated mainly on a single computer system.
- Data storage devices that generally use standard interfaces (IDE/ATA).
- Use of tools to easily recover deleted and allocated files.
- Introduction of DF courses at universities.

After 2007, in spite of the previous decade of rapid development, DF entered a crisis. This change was brought about by the development of fundamental changes in information technology such as:

- a sudden increase in the size of storage space, which is reflected in the scope and length of DF investigations;
- the number of different types of built-in flash units, which prevents device imaging;
- unlike in the previous period, the investigation often covers more networked devices;
- increased use of encryption, which prevents decryption of data in DF investigations;



* Accepted 25 March 2014.

- the use of cloud for storing data, which makes it much harder to image data;
- increasingly, malware is not stored on standard data storage (HD) and must be examined in RAM (RAM forensics);
- changes in legislation are frequent and are becoming a limitation factor for DF investigations; and
- DF syllabi and curricula are not standardized.

The rapid development of hardware and software, as well as issues concerning their security, demand a quick response through modern training, separately for each case: university education, new curricula and tools. Students following DF courses often complain that the subject is difficult to learn because it is multidisciplinary, with theoretical and practical knowledge fully intertwined. The fact that DF requires prior knowledge of other subjects (computer architecture, operating systems, computer networks, distributed systems, network security) was the initial idea for developing a virtual education environment with appropriate laboratories. The laboratory we developed and described in this paper applies project-based learning methodology that engages students in an integrating forensic theory with practice, and sees the big picture, rather than only pieces of the problem.

This novel virtual educational environment is designed for generic study of digital forensics. Our 3D Virtual Environment is ontologically described and implemented, using the composite-component model. The starting point was the idea presented in [6], which describes the concept of an academic program for digital forensics training. Based on this, we have created our own educational model with the following characteristics.

- Multidisciplinary content—in addition to technical knowledge of DF, investigators should have other skills such as a knowledge of the current legislation, expert testimony and cross-examination in court.
- Well-devised exercises—the exercises cover collection, storage, and handling of digital evidence.
- Highly qualified teachers—teachers should be experts in a given field, which is crucial for the success of the course; it is advisable to engage experts from various IT fields in the training.
- Real world examples—including a large number of real world cases from the recent past provides additional motivation for students.

The main features of our approach can be summarized as follows:

- a DF course based on virtualisation, visualization, and simulation using component composition model;
- fully integrated real and virtual environments;
- interactivity between students that work concurrently;
- adaptive and dynamic curricula;
- a project-based approach.

Students use labs for learning, pre-testing, testing and group work. The lab also helps professors to prepare experiments and assignments, administer lab experiments, and monitor student's progress during the course. Collaboration is an especially important part; it helps with elaboration, explanation, and evaluation of information in order to re- and co-construct new knowledge or to solve problems.

The entire composite-component model is placed in the 3D Virtual Environment that allows for easy monitoring of all events (temporal and spatial), while at the same time providing an opportunity for learning, testing and student–teacher interaction. The composite-component model enables case and scene searches, from the simplest to the highly complex combinations, as well as storage of complete scenarios and their reuse. After each semester, the gained experience is incorporated into new syllabi and curricula.

The paper is organized as follows. Section 2 discusses related work. Section 3 describes the virtual lab model with appropriate ontologies, followed by Section 4 that presents curriculum development. Section 5 explains the usage of the DF Lab through an example. Section 6 gives a preliminary assessment and evaluation of our approach, and Section 7 concludes the paper.

## 2. Previous research

Of particular importance for the topic of this paper are works discussing forensics in the field of academia (education and research). Authors of the paper [7] deal with the definition of a good agenda that could be used in forensic training (digital forensics education agenda). In the paper [8], a method in which virtual reality (VR) technology could be used to create a realistic environment for forensic training is presented. Authors of paper [9] explain the role of simulation in various aspects of teaching and training; the same authors in work [10] present a system for the education of digital forensic experts based on the Second Life simulation environment. In the paper [11] the authors created, administered, and implemented a learning laboratory for the application of digital forensics to the acquisition of digital materials. Work [12] reports on the state of the Falcone Programme and AGIS projects and looks at some of the innovative academic partnerships in the DF field. Paper [13] describes Cham-

plain College's online master's degree programme in Digital Investigation Management.

The paper [14] focuses on a virtual reality application utilising a design approach to produce an interactive prototype for the usage of visualization and reconstruction of forensic research. Marean et al. in [15] describe a digital forensic network lab, while work presented in [16] focuses on the technical aspects of digital forensics in distributed cloud environments. Researchers in [17] highlight the availability of a computing environment through the use of virtual machines, which can be helpful in acquiring the computing environment for forensic investigation.

In paper [18] the potential role of virtual environments in the analysis phase of computer forensics investigations is discussed. The research in [19] aims to identify differences in detection capabilities of honey pots deployed in two different environments (virtual machines and physical machines). In paper [20], the SVL model is used (Secure model for Virtualisation Layer). Paper [21] argues that investigation in the virtual environment is simpler than investigation in the physical environment.

There is a lack of scientific papers on the use of ontology in the field of digital forensics. Brinson et al. in [22] developed the cyber forensic ontology for the purpose of finding the correct level for specialization, certification, and education within the cyber forensic domain. Their ontological model can also be used for the purpose of curriculum development. Paper [23] presents Digital Investigation Ontology (DIALOG), which encapsulates all concepts of the digital forensics field and their relationships. In paper [24], a systematic mechanism entitled Digital Investigation Evidence Acquisition Model Based on Ontology Matching (DIEAOM) was proposed.

Many universities already have a DF course at undergraduate study level. However, this course is usually not followed by a corresponding advanced course at post-graduate levels. Also, we are facing the problem that curricula for DF courses are not yet standardized.

Compared with the previous research, our paper introduces a few key, novel ideas in the area of digital forensics education (Fig. 1).

- A cloud system and virtual machines used as the platform, and also as an integral part of forensic analysis.
- Digital forensics and higher education institution models are ontologically described; they are highly dynamic and can easily be expanded with new ontologies.
- The ontological model is of the composite-component type and, based on it, a 3D virtual education environment was implemented.
- The ontological model is used for curriculum development.

## 3. Virtual lab model

There are many reasons for using the 3D environment in teaching and learning, and some of the most notable according to [25] are:

- to facilitate familiarization of inaccessible environments;
- to facilitate task mastery by practising dangerous or expensive tasks;
- to improve transfer of knowledge by situating learning in a realistic context;
- to improve motivation through immersion;
- to reduce cognitive load through integration of multiple information representations;

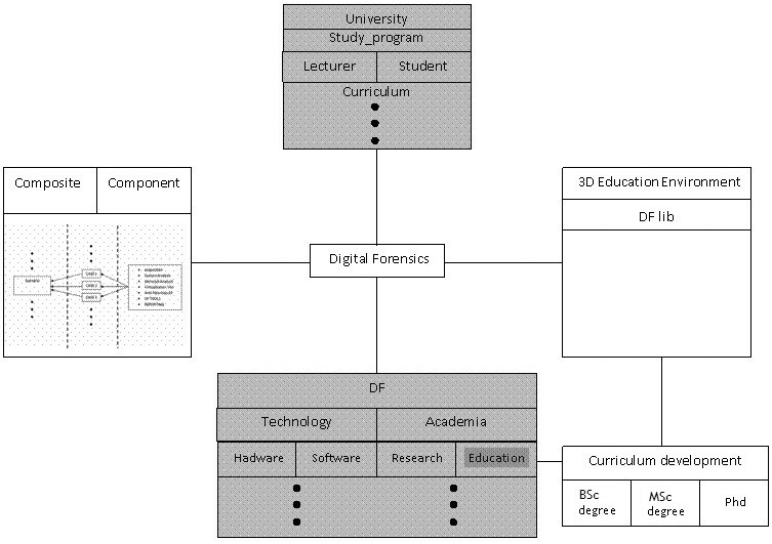


**Fig. 1.** The architecture of the DF model.

- to facilitate exploration of complex knowledge bases; and
- to facilitate understanding of complex environments and systems.

The benefits of using 3D environments in teaching can be demonstrated by various metrics: the number of students who take the course, the percentage passing the exam, the average grade, time management, and technical skills. Research proves that applying 3D improves the engagement of the students and their contextual and collaborative learning skills, and is especially useful in situations where spatial representation of knowledge is important.

Our virtual educational environment for teaching digital forensics has the following characteristics:

- it contains a set of rules that describe the behaviour of elements in an interactive, 3D environment;
- the formal ontology describes all elements contained within the environment;
- members of a group that uses the virtual 3D environment (students, professors) are also related to the ontology.

The 3D environment is organized as a digital forensics virtual lab, in which we first create the basic components—objects to be related, define new compositions, and finally place them all in a library. The ontology defines relations between all of the components and compositions.

Our system allows teachers to cover topics in digital forensic with practical examples and interactive work, and to verify students' work. Moreover, the teacher is able to analyse the log of students' activities; the value of a logging system is that it can provide answers to following [26].

- How much time do students spend within the classroom?
- How much material do they go through?
- In which order do the students study the topics?
- Are there pages/topics that students spend a lot more time on than others?
- Are there pages/topics that students skip?
- What is the average time that students spend on the application or page?
- Do the students take the default path or do they tend to study the topics in some other order?

### *3.1 DF virtual lab: physical implementation*

Our university uses virtual machines to teach a variety of information technology topics and courses. Many different operating systems can be demonstrated on a single student desktop requiring a short time for set up. The benefits to the students include more instruction and obtaining hands-on in a shorter period of time. Since our university signed a legal agreement with Microsoft allowing the use of their software for educational purposes, all our students can freely use different versions of the Windows operating system.

For the purpose of the lab assignments, we use virtual machines with different characteristics, and different numbers of instances. As for the operating system, the Windows 2012 server is used, and constitutes the core of the system; all of the necessary virtual machines are run through its virtualisation subsystem Hyper-V v3. Virtual machines are used for generating the student user interface, as well as server applications and delivery of educational materials. A number of virtual machines are created, configured, and placed in the virtual machine repository where they are registered and subsequently used to create laboratory instances, consisting of: Windows XP/VISTA/WIN 7/WIN SERVER, Linux/UNIX, Android simulator, iOS simulator, router iOS simulator, DEFT 7.2 live distribution, SIFT WORKSTATION 2.14 live distribution, BACKTRACK 5 R3 live distribution, Windows 2012 server with FTK, and ENCASE.

At first run of the lab, instantiation of virtual machines is carried out, which includes copying and customising each of the defined instances. Upon lab shutdown, virtual machines are frozen and, during subsequent launches of the lab, they are unfrozen.

A description of the hardware platforms used is as follows: server platform IBM System x3650 M3, with 2× Intel Xeon E5645 (6c/12t), 4×8GB ECC DDR3 1333MHz, 2×300GB 15K 6Gbps SAS 2.5″ SFF Slim-HS SED, 4×1TB 7.2K 6Gbps NL SAS 2.5″ SFF HS HDD, 2×1Gbps network card (load balancing).

On the software side, virtual 3D labs are implemented using free, Java-based open source toolkit Open Wonderland for creating collaborative 3D virtual worlds [27]. Within an Open Wonderland scene, students can communicate with audio, and share live applications and documents. This toolkit is chosen over other similar ones (e.g. OpenSim [28]) for three main reasons.

1. Complete extensibility: developers and graphic artists can extend its functionality to create entirely new worlds and add new features to existing worlds; drag-and-drop of 3D models is supported, while the application design is modular so that it can be relatively easily extended by developing plug-ins.
2. Tight integration of immersive, high-fidelity stereo audio: participants in a scene can hear other people present in a virtual space at high sound quality. Since voices or other sounds become softer as you move away from them, Open Wonderland easily supports multiple,

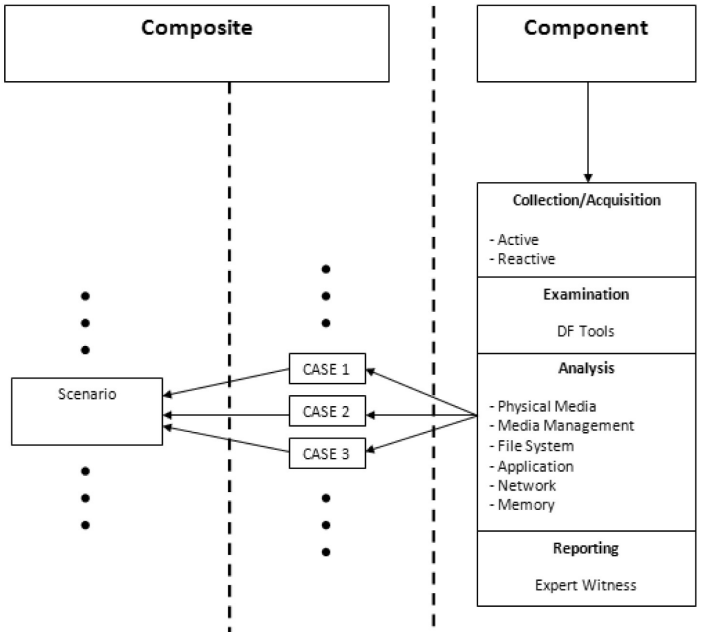


**Fig. 2.** Basic components and compositions in digital forensics.

simultaneous conversations within the same virtual space, something not possible with current audio or video conferencing technology.

3. Support for displaying remote desktops by using VNC (Virtual Network Computing) protocol. This way, we are able to display any previously described DF virtual machine configuration within the environment.

### *3.2 DF virtual lab: composite-component model*

The starting step in arranging the 3D DF Lab is to import basic 3D objects—components (referred to as cells in Open Wonderland). The library of basic components is then further extended by introducing new compositions (Fig. 2). This process implies relating and combining new 3D objects (3D composition components) into levels, as well as adding new functionalities and tools. Interactivity (referred to as capability in Open Wonderland) is then added to each object [29].

Typical students' activity in DF virtual lab follows a process model published by the US Department of Justice in the Electronic Crime Scene Investigation [30] that consists of four phases: Collection, Examination, Analysis and Reporting. Students apply this approach for self-learning, self-testing, and preparation for work in real life circumstances. To implement the Physical Crime Scene Investigation model, we use a physical lab with digital forensic hardware.

Virtual experimental equipment and materials need to be modelled into 3D entities. According to hierarchical analysis, 3D models are created first, and then composed into cases and scenes in a virtual lab. The virtual lab may be composed of many 3D entities and scenes, and can be extended. For a new experiment or lab, the user will select the necessary virtual entities and scenes from the virtual library and assemble them. The scene (composition) refers to the entire virtual lab, which stores many components and composites.

By combining various 3D entities, different cases are created, combined into scenes, and saved in a library. Virtual entity refers to an object that has properties and capabilities in an experimental scene.

Basic DF components are defined using Collection/Acquisition (active and reactive), Examination (DF Tools), Analyses (Physical media, Media management, File system, Application, Network and Memory management), and Reporting (Expert witness). These components constitute a case (for example: active DF acquisition, open source DF tools—Autopsy Forensic Browser, network analysis—Wireshark, and DF report). A scene is made up of many cases (for example: composition is made up of previously mentioned case and saved cases from the DF library). Several scenes can constitute a new case; combinations of scenes and cases are allowed.

We have attempted to create ontology (explicit specification of the conceptualization process) within the DF domain, for the purpose of finding the correct relations between education and research on one (academic) side, and hardware and software on the other (technology) side. Starting from the ontological model described in [34], we developed a hierarchical structure to serve for building 3D DF educational model. The first ontology we developed is DF ontology (Fig. 3); the

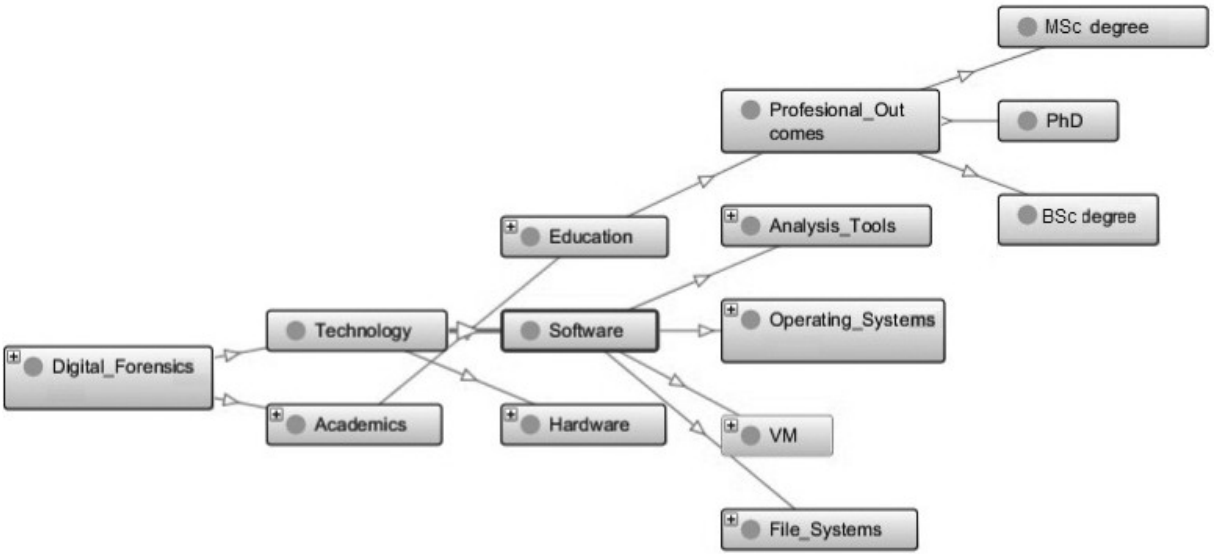


**Fig. 3.** Digital Forensics (DF) ontology.

second is the education institution ontology that is used for curriculum development. Both ontologies have been developed using the Protege editor [31].

### *3.3 DF virtual lab: example of composing a DF case*

Suppose that XXX is a company specializing in marketing services. It owns more than 50 computers, some of which are laptops, some desktops, and some tablet computers. It was observed that during the second half of 2012 certain information from the company network leaked. All computers are networked and use shared resources on the network for data storage. Also, a fast broadband connection to the Internet exists and some of the employees exchange data via Dropbox. It is suspected that one of the computers or online accounts for data storage has been compromised. It is surmised that the attack originated in the Dropbox Cloud System.

It is also important to emphasize that the company uses a 1 Gb wired network, as well as wireless networks, allowing for the possibility that someone had managed to break into the wireless network and thus gain access to the internal network. All networking equipment was produced by CISCO, and several CISCO routers exist with their own OS.

For the most part, Microsoft operating systems are used: on clients, these are Windows XP and Windows 7, while the servers use Windows 2008 Server. A RedHat Linux computer, used as a web server, also exists. For their needs, designers use Mac computers running iOS 6, while the majority of tablet computers run Android 4.1 OS, except for a few of the designer tablets that run iOS (iPad2).

Suspicious computers have been located and it is necessary to implement a full DF investigation. The task is to examine where the breach has occurred, to locate the source of the leak and to submit a detailed report as soon as possible to company management.

It is important to have in mind that an internal investigation is conducted here, as opposed to an official law enforcement investigation; this fact influences goals and requirements of the investigation.

The required steps for this case study are:

- acquisition of all computers and devices (live and classic), using either DEFT or SIFT distribution, as well as a command line tool that can be used for this purpose (e.g. DD, FTK Imager);
- forensic analysis of acquired data (Windows, Linux, Mac OS X, Android), using available tools inEnCase and FTK tools or the SIFT distribution;
- analysis of networks and network services (Cloud–Internet, network and router forensics), using tools to analyse network traffic and trace analysis of Internet service usage;
- repetition of the previous steps in the virtual environment and checking if the same or a similar solution exists in the Forensic Library;
- taking advantage of the virtual environment for interaction—cooperation (provided that students work in groups);
- preparing the forensic report; and
- saving the last scenario and report in the Forensic Library within the virtual lab.

The appearance of the Open Wonderland exercise with all the components that make up a scene is shown in Fig. 4.

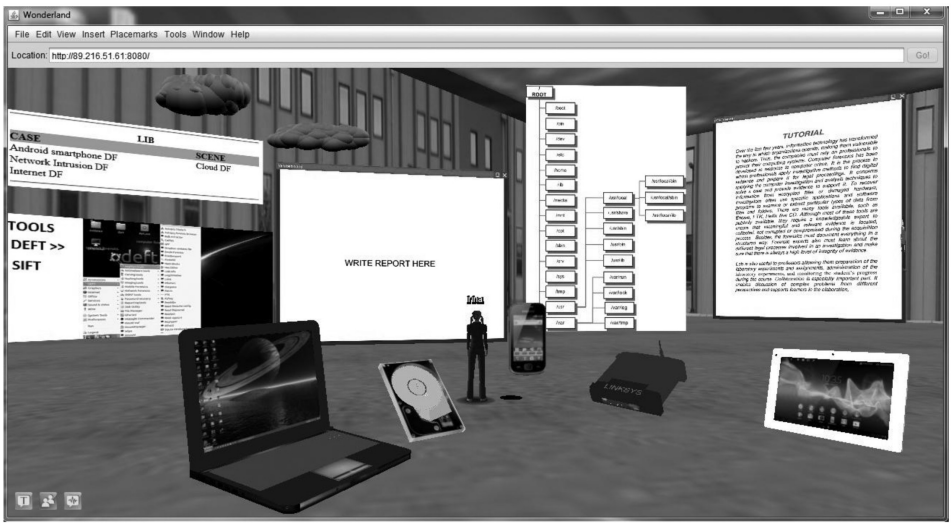


**Fig. 4.** Forensic scenario in Open Wonderland.

Figure 5 illustrates decomposing the scene to a library of components; in this particular case, the laptop has a teleporting capability through which a 3D scene participant can be directed to different placemarks (library components), which make up the scene.

## 4. Curriculum design

### *4.1 Ontology for curriculum development*

The general model of a higher education institution is shown in Fig. 6.

The ontology for DF in a higher education institution is defined by the following classes: University, Study_Programme, Student, Lecturer, Student_Course, Curriculum, Course, Semester, School_Year, DF_Syllabus, Composite, Component, Case and Scene. These classes represent natural concepts common to educational institutions. Classes contain a set of instances; for example, SingidunumUniversity is an instance of the class university. The ontology also contains relations that indicate natural relationships between objects in the real world. Classes are further developed into subclasses.

The university has many study programs; for each program, appropriate curricula and syllabi for DF are defined. The composite-component model is used with appropriate scenes and scenarios. At the same time, relations between students, lecturers, and university management are defined.


**Fig. 5.** Decomposing the scene into library of components; the left-hand side panel is used as a portal to direct students to different scenes that can be composed inside the 3D environment.

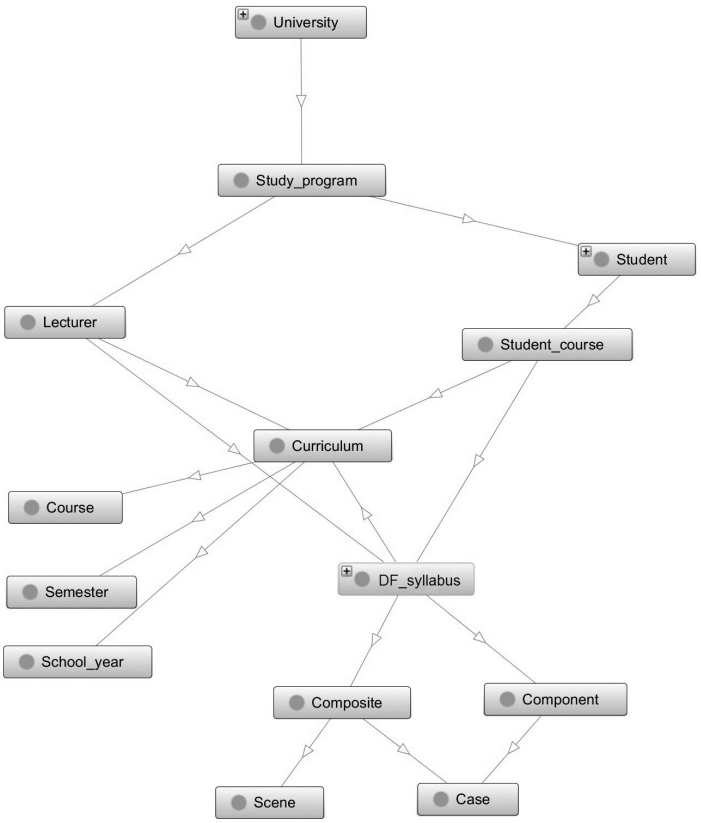


**Fig. 6.** Higher education institution ontology for curriculum development.

The model basically includes curriculum development for an undergraduate (four-year) degree, master degree, and a Ph.D. degree. This model can be used to assemble DF courses and course material.

### *4.2 DF syllabus for undergraduate studies*

The presented ontological model can also be used for curriculum development. To be able to follow the DF course, students are required to have previous knowledge from the following courses:

- Introduction to Computer science
- Operating systems
- Computer networks
- Computer security basics.

In our university, DF field is taught in an undergraduate course during the sixth semester of study. The duration of the course is one semester, or exactly 15 working weeks, 12 of which are intended for lectures and exercises, 2 for regular preliminary exams, and one, the last week, for make up of preliminary exams. An overview of the twelve-week lecture program is given below:

*1. Forensic acquisition—Classic/Live*
During the introductory lecture, students are introduced to the main concepts of a DF investigation, procedures to adhere to while conducting an investigation, and the study of classic data acquisition techniques (reactive forensics) for various types of devices (desktop, laptop, PDA/tablet/smartphone). Students are introduced to data acquisition techniques used on a running computer (active forensics), depending on the conditions (local live response, remote live response, and hybrid live response). During this week, students are also taught the correct sequence of data acquisition from a computer and the ways to handle the collected data.

*2. Media and file system forensics*
In the second week of lectures, students are introduced to the specifics of various file systems that may be encountered in DF investigations of computers, tablets or smartphones. All major file systems are covered (NTFS, FAT/FAT32, EXT2/EXT3, RAISERFS, YAFFS, HFS +, HFSX). During this week, students are also introduced to physical devices from which data are acquired and taught how to calculate the actual capacity of a particular media (disk geometry). Students examine aspects of digital media with an emphasis on understanding the advantages and limitations of using digitally produced data, and various ways in which digital data can be enhanced. Areas covered include SD/MMC card forensics, USB FLASH/NAND forensics, SSD forensics.

*3. Internet/Network forensics*
In the third week of lectures, students are introduced to Internet forensics, i.e. methods of data acquisition from a computer connected to the Internet (Internet artefacts). The areas covered include mail forensics, browser forensics (History, Cache, Searches, and Downloads), and chat client forensics (Facebook Live, MSN Messenger, Yahoo, AIM, GoogleTalk chat). In addition, during this week, students are also instructed how to analyse log files. Students are introduced to network forensics, i.e. methods used to acquire data related to a computer network and various mobile services. The areas covered include network monitoring/sniffing [32], network logs, and router forensics.

*4. Windows OS forensics*
In the fourth week of lectures, students are introduced to Microsoft Windows operating systems, i.e. methods of collecting various types of data from Windows OS. Students are introduced to Windows operating systems and taught how to analyse the registry database on Windows systems (Windows XP, Windows 7, Windows 2008 Server).

*5. Linux/Unix OS forensics*
In the fifth week of lectures, students are introduced to Linux/Unix operating systems, i.e. methods of collecting various types of data from Linux/Unix OS. Students are introduced to the specifics of Linux/Unix operating systems and taught how to analyse distributions (Ubuntu, Fedora, RedHat).

*6. Preliminary exam 1*
In this week students have the first knowledge test with two parts: theoretical and practical. The theoretical part consists of a quiz with 30 questions from lessons taught in the first five weeks; the practical part of the exam is to demonstrate skills in acquiring data from different types of media and the Internet in a forensic case developed within the virtual DF Lab. The maximum score on this part of the exam is 30 points (10 for the theoretical part, and 20 for the practical part of the exam). Exam duration is 90 minutes; 15 minutes for the quiz, and the rest of the time for completing the assignment in DF virtual lab.

*7. Smart phone forensics*
In the seventh week of lectures, students are introduced to the smart phone operating systems, i.e. methods of collecting various types of data from different smart phone OSs. The areas covered are Android forensics and Apple iOS forensics. Students are introduced to the specifics of different smart phone operating systems and taught how to analyse the smart phone.

*8. VM forensics*
In the eight week of lectures, students are introduced to virtualisation techniques and methods of virtual machine investigation, as well as methods of using a virtual machine as a forensic tool. This part covers the commonly used environments, namely: VMWare, Microsoft Hyper V and Oracle VirtualBox. Students are also introduced to the specifics of data acquisition from running virtual computers and the specific method of acquiring data using the Suspend mode of the virtual machine.

*9. Anti-forensics*
In the ninth week of lectures, students are introduced to anti-forensic techniques and frequently used tools. Covered areas include: data hiding, encryption, steganography, artefact wiping, trail obfuscation, attacks against computer forensics. During this week, in addition to the introduction to different types of anti-forensic techniques and tools, students are also introduced to methods of using virtual machines and live distributions to hide traces of offences committed. This topic is devoted to artefacts left behind by anti-forensic techniques (anti-anti-forensics).

*10. Forensic tools 1—open source*
In the tenth week of lectures, students are introduced to free and open source tools and distributions that contain various tools relevant for DF investigations. Students are introduced to two of the most popular distributions for DF investigations, namely DEFT 7.2 and SIFT WORKSTATION 2.14, as well as the most popular hacker distribution BackTrack 5 R3, and tools available in these distributions (AUTOPSY/SLEUTH KIT, DFF, PyFlag).

*11. Forensic tools 2—commercial*
In the eleventh week of lectures, students are introduced to commercial tools and their capabilities in a DF investigation. In particular, students are introduced to two of the most popular tools for DF investigations: FTK 4 and AccesDataEnCase v7. Students learn how to apply these tools in areas of collection and analysis of data acquired using one of the previously learned techniques.

*12. Preliminary exam 2*
In this week students have the second knowledge test, which has a theoretical and a practical part. The theoretical part is a quiz containing 30 questions covering lessons from previous weeks, and a practical forensic case in the DF virtual lab where students must demonstrate forensic skills in areas of smartphone forensics, virtual machines, anti-forensics, and using different forensic tools. The maximum score on this part of the exam is 30 points (10

for the theoretical part, and 20 for the practical part of the exam). The exam duration is 90 minutes; 15 minutes for the quiz, and the rest of the time for completing the assignment in the DF virtual lab.

*13. Hybrid and emerging technologies forensics*
In the thirteenth week of lectures, students are introduced to Cloud Forensics, Social Networks, Data Warehouse, Control Systems (SCADA), Critical Infrastructure, Virtual/Augmented Reality. Students are also introduced to the specifics of data acquisition from such systems.

*14. Reporting/ Expert witness*
In the fourteenth week of lectures, students are introduced to rules on proper report preparation and recommendations that may arise as a result of years of experience in the field of expert testimony on DF investigations. Students are also taught the rules of giving evidence, i.e. giving expert testimony in court (cross-examination) and expertise. Within the DF virtual lab a virtual courtroom is used, where students learn how to properly present the results of a DF investigation.

### *4.3 DF syllabus master degree*

The first step in analysing the programs listed in the related work section involved the DFCB (Digital Forensics Certification Board) domains [32]. We focused on works tackling the development of a standard digital forensics master's curriculum, such as Beebe and Clark's knowledge domains [33] and paper [34]. We also analysed the current master curricula across the US Universities.

Based on the findings of the mentioned authors, as well as key areas that should be covered, we defined the following M.Sc. curriculum, specifically tailored to our needs; this is a direct sequel of the undergraduate studies curriculum:

- Advanced Host-Based/Hypervisor Forensic Analysis
- Advanced Network/Cloud Analysis
- Advanced Research Topics in Cyber Forensics
- Event Reconstruction and Correlation
- Hacking Exploits and Intrusion Detection
- Malware and Software Vulnerability Analysis
- Network Security, Data Protection and Telecommunication
- Legal Aspects of Digital Investigations
- Digital Forensics Research/Forensic Sciences Practicum
- Internship.

### *4.4 DF Ph.D. syllabus*

On the basis of our experience with master curricula, the following curriculum was created that is specifically tailored to our needs.

- Programming digital forensic analysis: a course which focuses on writing special purpose programs for analysing digital evidence. It includes laboratory exercises ranging from the creation of a simple shell and scripts to the customisation of special purpose programs for use in forensic analysis.
- Challenges to digital forensic evidence.
- Research methods: a course which focuses on qualitative and quantitative research methods in the digital forensic virtual lab.

## 5. Evaluation

We use our own teaching and course evaluation system to measure students' attitude towards a course, the materials included in the course, and the 3D DF Lab. Our approach is described in [35]. At the end of the course, anonymous online student surveys are conducted to determine whether the learning outcomes have been successfully achieved. Questionnaire includes specific questions on the use of the DF Lab and course projects. Students are asked questions related to their personal opinions and experiences and the course effectiveness in terms of programme and course outcomes. The five possible answers are rated from 1 to 5: Strongly disagree, Disagree, Undecided, Agree and Strongly agree. Students are also allowed to write specific comments, as the process of assessment is anonymous and voluntary. This instrument was used to evaluate students' interest in the newly developed materials (and virtual 3D DF Lab) and to find out whether or not they consider the materials useful and helpful. In total, nine out of 12 students participated in the process. The average rating calculated from the nine responses gathered was 3.64 (agreeing more than being undecided). Moreover, most of the answers cluster around 4 (Agree), which shows a uniform opinion distribution among students.

In order to evaluate more closely the effect of introducing a 3D virtual DF Lab, students were asked to rate their impressions. Table 1 shows the students' feedback on the difficulty of the exercises and the effect of the DF Lab on learning and interest in the topics covered by the exercises.

Students added several comments to the survey, indicating that this approach is an excellent way to learn material because simulation can provide answers to many practical questions. Students were given the opportunity to state which options are missing from the system, and which options should be implemented in a different way. Negative

**Table 1.** Students' feedback on the difficulty of the exercises and the effect of the DF Lab on learning and interest in the topics covered by the exercises

| | Difficulty of the material (1 = easy, 5 = hard) | Effect of DF virtual lab on learning (1 = none, 5 = significant) | Effect of DF virtual lab on interest (1 = none, 5 = significant) |
|---|---|---|---|
| Forensic acquisition | 3.1 | 3.4 | 3.6 |
| Media and file system Forensics | 4.1 | 3.8 | 4.0 |
| Internet/Network forensics | 3.3 | 4.1 | 4.7 |
| Windows OS forensics | 3.8 | 4.6 | 4.5 |
| Linux/Unix OS forensics | 4.5 | 4.5 | 4.3 |
| Smart phone forensics | 4.3 | 4.7 | 4.6 |
| VM forensics | 4.0 | 4.6 | 4.3 |
| Anti-forensics | 4.7 | 4.3 | 4.8 |
| Forensic tools 1—Open source | 3.6 | 4.2 | 4.4 |
| Forensic tools 2—Commercial | 3.4 | 4.2 | 4.6 |
| Hybrid and emerging technologies forensics | 4.1 | 4.1 | 4.2 |
| Reporting/ Expert witness | 2.9 | 3.9 | 3.7 |

comments mainly include the time required to gain a grasp of the movement in the 3D environment, because not all students had experience with gaming environments. Generally, assessment indicated that students' perception of the DF Virtual Lab is positive, with a satisfied sense of reality, which encourages its further developing.

Our virtual forensic lab is currently used as a teaching aid. The surveying of students is conducted periodically, with questions that cover only the method of using the virtual education environment and possible suggestions and comments to improve any of the components: graphical interface, content, tutorial, communication, operation speed. Student feedback is used not only for changes to the virtual education environment, but also for adapting curricula and syllabi. Suggestions and comments from students are tracked separately for each semester. Based on gathered experience, we are endeavouring to create a complex virtual education model with a general application, one that could easily be applied to various fields of research and education.

It may be argued that the greatest strength of our method is at the same time its weakness: to be effective and to use all the advantages of a collaborative approach to their full extent, the virtual lab can be used by only a limited number of students. Therefore, this approach is not applicable to traditional course organization. Also, students must spend some time learning to use the virtual classroom, but once mastered, new skills begin to pay off immediately, as confirmed by our students' survey.

## 6. Conclusions and future research

In this paper, we have introduced and described the process of developing a 3D lab, ontology, and curriculum for undergraduate, M.Sc. and Ph.D. courses in digital forensics.

Preliminary results indicate that students benefit from using 3D environment in terms of interest in the subject, confidence in the materials provided, and the ability to understand and use the presented techniques. Instructors and students can create their own virtual lab set-ups with various components for teaching and learning DF concepts.

Although the developed 3D DF Lab is currently used only as an auxiliary course component, the next logical step will be to introduce the virtual lab as an everyday means of teaching, and to automate all the procedures involved by applying artificial intelligence. Our goal is to develop a self-learning environment, capable of tracking students' learning profiles and statistics on virtual lab usage, generating conclusions and rules for adjusting syllabi and curricula. It is our strong belief that in the future all educational institutions will adopt virtual environments to various degrees, and this paper presents our experiences in promoting this approach in DF education.

This paper also describes the development of the DF course curriculum for all three levels of university studies: undergraduate, Masters, and Ph.D. We surveyed available curricula from the most renowned universities and formed a proposal that also takes into consideration our significant experience in teaching DF at various levels of study. The proposed curriculum is original and we believe that it can be of use to others as a guidance.

*Acknowledgement*—The work presented here has been supported by the Serbian Ministry of Education and Science (project grant no. III44006).

## References

1. Encase homepage, http://www.guidancesoftware.com/encase-forensic.htm, accessed June 2013.
2. FTK homepage, http://www.accessdata.com/products/digital-forensics/ftk, accessed June 2013.
3. SIFT homepage, http://computer-forensics.sans.org/community/downloads, accessed May 2013.
4. DEFT homepage, http://www.deftlinux.net, accessed June 2013.

5. Helix homepage, http://www.e-fense.com/products.php, accessed May 2013.
6. C. Taylor, B. Endicott-Popovsky and A. Phillips, Forensics education: assessment and measures of excellence, *Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07)*, Bell Harbor, WA, 2007, pp. 155–165.
7. M. Al Falayleh, Building a Digital Forensic Laboratory for an Educational Institute, The International Conference on Computing, Networking and Digital Technologies (ICCNDT2012), Bahrain, 2012, pp. 285–293.
8. K. Nance, H. Armstrong, C. Armstrong, Digital forensics: defining an education agenda, *43rd Hawaii International Conference on System Sciences*, 2010, pp. 1–10.
9. J. Crellin, S. Karatzouni, Simulation in digital forensic education, *Third International Conference on Cybercrime Forensic Education and Training (CFET3)*, 2009.
10. J. Crellin, M. Adda, E. Duke-Williams, J. Chandler, Simulation in computer forensics teaching: the student experience, *Researching Learning in Immersive Virtual Environments*, 2011.
11. A. C. Lee and K. Woods, *Digital Acquisition Learning Laboratory: A White Paper*, School of Information and Library Science University of North Carolina at Chapel Hill, 2011.
12. P. Stephens and A. Induruwa, Cybercrime investigation training and specialist education for the European Union, *Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007)*, 2007, pp. 28–37.
13. C. G. Kessler and D. Haggerty, Pedagogy and overview of a graduate program in digital investigation management, *41st Annual Hawaii International Conference on System Sciences*, 2008, pp. 481.
14. E. Soon Eu Hui, R. Hedley and D. Leva, Interactive 3D forensic visualisation: virtual interactive prototype, *Computer Graphics, Imaging and Visualisation*, 2007, pp. 148–153.
15. S. J. Marean, M. Losavio and I. Imam, A research configuration for a digital network forensic lab, *Third International Workshop on Systematic Approaches to Digital Forensic Engineering*, 2008, pp. 141–142.
16. D. Birk and C. Wegener, Technical issues of forensic investigations in Cloud computing environments, *Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE)*, 2011, pp. 1–10.
17. S. Zawoad and H. Ragib, *Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems* (arXiv preprint arXiv:1302.6312), 2013.
18. D. Bem and E. Huebner, Computer forensic analysis in a virtual environment, *International Journal of Digital Evidence*, **6**(2), 2007.
19. J. Narvaez, C. Aval, B. Endicott-Popovsky, C. Seifert, K. A. Malviya and D. Nordwall, Assessment of virtualization as a sensor technique comparison of detection capabilities of honeypots deployed in virtual environments versus physical machines, *Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering*, 2010, pp 61–65.
20. S. Manavi, S. Mohammadalian, N. Izura Udzir and A. Abdullah, Secure model for virtualization layer in Cloud infrastructure, *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, The Society of Digital Information and Wireless Communications, 2012, pp. 32–40.
21. V. S. Khangar, E. Nagpur and R. V. Dharaskar, Digital forensic investigation for virtual machines, *International Journal of Modeling and Optimization*, **2**(6), 2012, pp. 663–666
22. A. Brinson, A. Robinson, M. Rogers, A cyber forensics ontology: creating a new approach to studying cyber forensics, *Digital Investigation*, Volume 3, supplement, 2006, pp. 37–43.
23. D. Kahvedzic and T. Kechadi, DIALOG: A framework for modeling, analysis and reuse of digital forensic knowledge, *Digital Investigation*, 6, 2006, pp. S23–S33.
24. J. Huang and A. Yasinsac, Knowledge sharing and reuse in digital forensics, *Fifth IEEE International Workshop Systematic Approaches to Digital Forensic Engineering (SADFE)*, 2010, pp. 73–78.
25. B. Dalgarno, S. Gregory, L. Carlson, M. J. W. Lee and B. Tynan, A systematic review and environmental analysis of the use of 3D immersive virtual worlds in Australian and New Zealand Higher Education Institutions, Final Report, dehub Report Series, Armidale NSW, University of New England, Australia, 2013.
26. J. Heywood, *Engineering Education: Research and Development in Curriculum and Instruction*, Wiley–IEEE Press, 2005, pp. 391–415.
27. J. Kaplan and N. Yankelovich, Open Wonderland: Extensible Virtual World Architecture, *IEEE Internet Computing*, **15**(5), 2011, pp. 38–45.
28. OpenSim homepage, http://opensimulator.org, accessed June 2013.
29. I. Branovic, D. Markovic, R. Popovic, V. Tomasevic and D. Zivkovic, Development of modular virtual lab for introductory computing courses, *IEEE Global Engineering Education Conference (EDUCON)*, Berlin, Germany, 2013, pp. 1027–1031.
30. NIST—National Institute of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders*, http://www.ncjrs.org/pdffiles1/nij/187736.pdf
31. Protégé homepage, http://protege.stanford.edu, accessed June 2013.
32. DFCB, http://www.ncfs.org/dfcb/DFCB_Final_KSAs-submited-3-15-2009.pdf, accessed June 2013.
33. N. L. Beebe and J. G. Clark, Digital forensics curriculum development: Identification of knowledge domains learning objectives and core concepts, *Proceedings of the Twelfth Americas Conference on Information Systems*, paper 421, Acapulco, Mexico, 2006.
34. Kathleen Strzempka, The development of a standard digital forensics master's curriculum, College of Technology Masters Theses, Purdue University, 2010.
35. M. Zivkovic, B. Nikolic and R. Popovic, eWISENS: Educational Wireless Sensor Network Simulator, *International Journal of Engineering Education*, **30**(2), 2014, pp. 483–494.

**Igor Franc** received his B.Sc. and M.Sc. degrees in computer science at the Singidunum University of Belgrade, Serbia, and is currently pursuing his Ph.D. degree in the Digital Forensics at the Faculty of Informatics and Computing, Singidunum University of Belgrade. He is currently a teaching assistant in the Department of Informatics and Computing, Singidunum University of Belgrade. His research interests include digital forensic, databases, operating systems, computer networks, computer security and distance learning.

**Ivan Stankovic** received his B.Sc. degree at the Faculty of Management from Novi Sad, in 2005, his M.Sc. degree at the Faculty of Informatics and Computing, Singidunum University, in 2008, and is currently pursuing his Ph.D. degree at the Faculty of Informatics and Computing, Singidunum University. He is currently a Lecturer at the Business School of Applied Studies from Blace, Serbia. His research interests include semantic web, big data, Internet programming and programming language Java.

**Irina Branovic** received her B.Sc. and M.Sc. degrees in electrical engineering from the School of Electrical Engineering, University of Belgrade, Serbia, and her Ph.D. degree from the University of Siena, Italy. She is currently an Associate

Professor in the Department of Informatics and Computing, Singidunum University, Belgrade. Her research interests include computer architecture, Internet/Java programming, and distance learning.

**Ranko Popovic** received his B.Sc. degree in electrical engineering at the University of Pristina, in 1980, his M.Sc. degree in electrical engineering at the University of Nis, in 1988, and his Ph.D. degree in electrical engineering at the University of Pristina in 1996. He is currently a Professor of computer engineering at the Faculty of Informatics and Computing, Singidunum University, Belgrade, Serbia. His research interests include operating systems, computer networks, wireless sensor networks, multimedia systems and distance learning.