PERFORMANCE AND STUDENT PERCEPTION EVALUATION OF CLOUD-BASED VIRTUALISED SECURITY AND DIGITAL FORENSICS LABS

Prof William J. Buchanan[1], Dr Jamie Graves[1], Niladri Bose[1], Bill Buchanan[2], Richard MacFarlane[1], Robert Ludwiniak[1], and Brian Davison[1]

[1]School of Computing, Edinburgh Napier University, UK

[2]Dell UK, Glasgow, UK

Abstract — **This paper focuses on the integration of virtualised environments within the teaching of computer security and digital forensics, and includes three case studies. It stresses the importance of students working on real-life environments, through virtualized infrastructures, in order to improve their skills so that they are more employable. The first case study involves assessing student perception on the usage of VMware Workstation and AWS (Amazon Web Services) for security and digital forensics labs, while the other two present a performance and reflective evaluation of a Cloud-based infrastructure using VMware ESXi. The evaluation for the first case study shows the results of a questionnaire for the integration of VMware Workstation and AWS, and highlights that the virtualised environment seems to engage students more than traditional desktop ones, along with identifying the key areas which seem to be useful, such as for network forensics and in running instances within a sand-boxed environment. The other two case studies show an evaluation of the performance impact of security and digital forensics students using a Cloud-based infrastructure for their labs, and that the developed infrastructure copes well with both scheduled lab-based classes, remote access, and a virtualised environment for courseworks.**

1. Introduction

Most computing modules often require some form of lab-based practical work, as this can considerably enhanced the employability of the students. Unfortunately, these labs can be fairly limited in their scope, as they must be run on a standard academic desktop. Along with this, it is often difficult for students to complete their lab-based work remotely, or provide an equivalent infrastructure within franchised programmes. Thus the usage of virtualised labs have a great potential, as students can get the same lab infrastructure as local students would get in the lab, and also operate within a sand-boxed environment, where they can take full control of their environment.

In terms of security and digital forensics teaching there are many additional advantages to virtualisation, including allowing students to learn on systems which are near to real-life, and which are within a ring-fenced and sand-boxed environment. This allows for a wider range of security tools to be used which would not normally be allowed on computers within a traditional lab-based environment. Tools such as hping [2], which allows TCP packets to be crafted, such as when creating SYN floods, can thus be used within a fenced environment, and where students cannot access hosts outside the environment. In terms of digital forensics, student can train on systems which are complete, and analyse them

for both static and live forensics. Virtual images can then be setup with a number of scenarios, and students can mount drives for static analysis, or analyse running systems for live forensics.

Other associated benefits for tutors include the enhanced support for remote/distance learning, and the easy setup/modification of labs. There are, though, still many key questions that remain on the usage of virtualised environments within security and digital forensics, including:

- Whether students actually prefer the virtualized environments to a normal desktop installation?
- Whether typical cluster infrastructures can cope in terms of performance for normal student usage (including peaks in load caused by coursework assessments)?
- Whether public cloud infrastructures are better than private ones?
- What the typical usage of the virtualized infrastructure will be?

This paper aims to provide some evidence on the answers to these questions, and is part of on-going work to fully answer them, and if they can be answered, the employability of the students can be considerably enhanced.

2. Background

Figure 1 outlines the different infrastructures that can be used within a cloud-based architecture. This includes using a public cloud infrastructure such as Amazon Web Services (AWS), for a pay-as-you-go model. Using AWS allows for a robust and scalable infrastructure, where all of the virtualised desktops exist outside the educational environment, and thus has a reduced risk of downtime. It is thus useful, in an academic environment, for many computing related subjects, especially in database development and in teaching operating systems. The teaching of security and digital forensics might, though, be difficult for ethical issues, especially in using certain types of software, such as using NMAP to discover the services on a host. The best approach might thus be for a private cloud infrastructure, which is run by the academic organisation, or for a community cloud, where academic institutions could share their cloud infrastructure, but keep them within a private environment.

The running of desktops within a cloud infrastructure obviously has risks, especially in providing a 100% uptime (which is often difficult in academic environments, especially

outside normal working hours), and in terms of performance (as poor performance, such as for system lags). Thus the stand-alone environment, such as for VMware Workstation and VMware Fusion, offer an excellent back-up, where the same VM image can be used locally on a standard PC, as is run within the cloud. Thus if there is a problem with the connection to the cloud, the student can use the same environment using the stand-alone version. The major problem with this, though, is that students cannot collaborate across different hosts, without a fairly complex network configuration. The students can also struggle to get a copy of the instance for their home computer (although USB storage disks now have a fairly high capacity, and are fairly inexpensive). Figure 2 outlines the basic choices for virtualisation.

Figure 3 shows the three main environments used within this paper for the teaching of security and digital forensics labs. This includes using a stand-alone virtualisation environment such as VMware Workstation/Fusion to run instances, and with VMware ESXi and AWS to create a private and a public cloud, respectively. The VMware software is available to academia from the VMware Academy Programme, and AWS through an AWS Teaching Grant.


Figure 1: Cloud infrastructures

Figure 2: VM instances
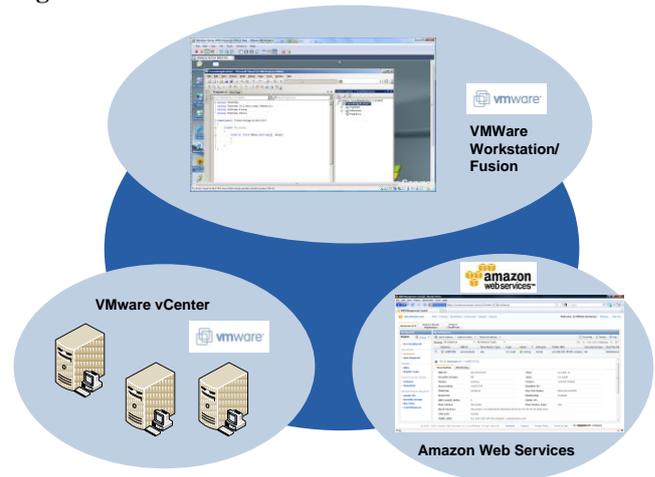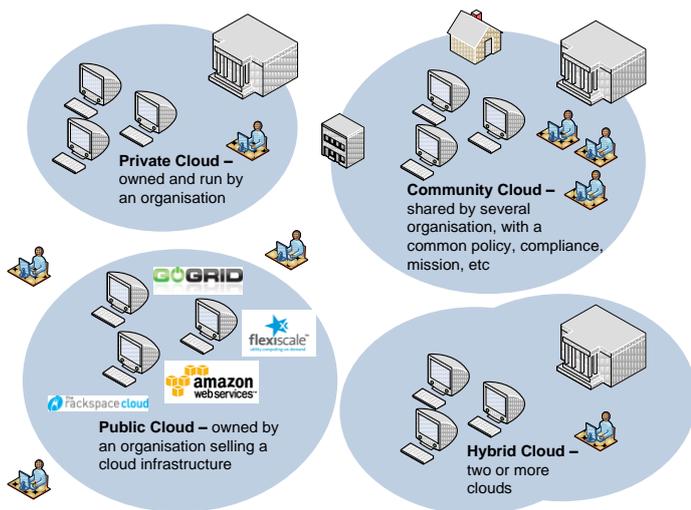
Figure 3: Alternatives
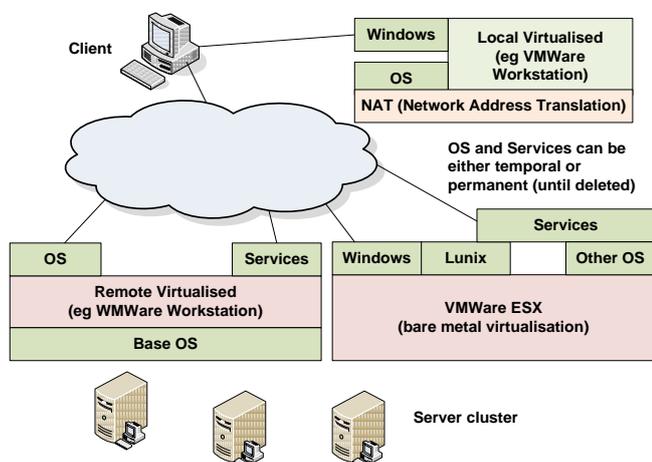
3. Private Cloud infrastructure

Case Study 1 uses VMware Workstation and AWS to determine students' perception on virtualisation, whereas Case Studies 2 and 3 use a private cloud based on VMware ESXi, as shown in Figure 4. Several other options were evaluated for the cloud infrastructure, including the Ubuntu cloud, but these have often been difficult to use within a teaching environment, whereas VMware vCenter has the complete management infrastructure for controlling users and instances (and is available though the VMware Academic Programme [1]).

The developed infrastructure has three main ESXi hosts (Socesx2, Socesx4 and Socesx3), and a main controller (Socesx1). The main controller runs: Lab Manager (which provides a Web browser interface which students connect too, to run their instances); a firewall/router (which allows certain types of traffic to be blocked, and a routing between the private internal network and the external one); a shared data storage of 4TB (using iSCSI for fast access times); and vCenter (which is responsible for controlling the ESXi hosts). A large shared storage is important as hundreds of instances need to be stored, and along with this a relevantly large memory is often required on the cluster hosts in order for them to run many instances at a time without extensive need for disk caching. While the controller does not have to be a particularly powerful computer, it is important that the clustered hosts can perform well, so the two main cluster servers (Socesx2 and Socesx3) were selected with the following specification:

Type:	Dell PowerEdge R410
CPU:	Intel Xeon 2.27GHz, 8CPUs (16 logical processors on two physical processors)
Licence:	vSphere 4 Advanced
Memory:	32GB

Each of the cluster hosts has two network connections, one which connects to an internal private network and the other to a router/firewall running on the controller. The internal

network has been set for 192.168.x.x/16, which allows for more than 65,000 virtual hosts to be created, and which can be shared on the same network (this is important as it allows students to work together and use each other instance for security evaluations). The router on the controller then allows for external connections to the public network. For security and digital forensics modules this connection should be used only for transferring files (such as screen shots taken within the images) or in downloading software.

For the Semester 1, 2010 session (Sept-Dec 2010), the cluster was setup so that the first server (Socesx2) takes most of the loading, and, when it is too busy, the second server takes some of the loading, and so on. The modules which ran on the cluster were: **Host-based Digital Forensics** (with eight students for a scheduled two-hour lab); **Security and Forensic Computing** (with an average of 25 students per session, for two two-hour session); and **Database for Business** (with an average of 20 students per session for a two-hour weekly session).
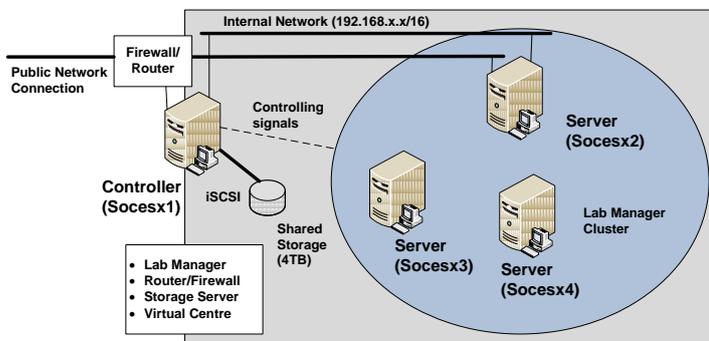

Figure 4: VMWare ESXi infrastructure

4. Case Study 1 (Advanced Security and Digital Forensics)

The first case study investigated student perceptions of a range of virtualised infrastructures for computer security and digital forensics labs. It was run over Semester 2, 2010 (Jan-Jun 2010), and used Amazon Web Services and VMware Workstation to provide virtualised desktops [3,10]. The module uses virtualised labs including:

- Windows 2003 Services and Penetration Testing.
- UNIX Services and Penetration Testing.
- SQL Injection.
- Network Forensics.

The coursework was based around a simulated malicious activity where the network traffic was captured and stored within a VM image, which also contained the host activity of the event. This included the upload of files through FTP activity. Students were then tasked to make a judgement of the sequence of activities on the host, and to match up network traces with host-based traces (such as with event logs or within the file structure).

Table 1 summarizes the results of an anonymised survey, taken from a 20% sample of a class size of 70, for the

VMware stand-alone instances. It can be seen that overall that it was a success within the coursework, and in investigating different operating systems, but not as strong in creating real-life environments.

Table 1: VMware results (e.g. SD - Strongly disagree)

	SD (%)	D (%)	Neu-tral (%)	A (%)	SA (%)
VMware helped me to undertake an in-depth study of the host in the coursework	0	0	0	22	78
VMware helped me to undertake an in-depth study of the network traffic in the coursework	0	0	33	22	33
For VMware images, they allowed you to setup a wide range of operating systems.	0	0	0	33	67
For VMware images, they supported lab setups which were already pre-prepared.	0	0	0	67	33
For VMware images, they gave me experience of using real-life operating systems.	0	0	22	33	44
For VMware images, they allowed me to study remotely.	0	0	0	56	33
For VMware Images, they allow the usage of tools within a sandboxed environment.	0	0	11	44	44

The results for AWS, as given in Table 2, shows that it was less successful than the stand-along environment, but it did allow students experience of a real-life cloud infrastructure.

Table 2: AWS results

For AWS, it allowed me to setup a wide range of operating systems.	0	0	0	56	44
For AWS, it supported lab setups which were already pre-prepared.	0	0	22	44	33
For AWS, it allowed experience of using real-life cloud infrastructures.	0	0	0	33	67
For AWS, it allowed me to study remotely.	0	0	33	33	33
For AWS, it allowed the usage of tools within a sandboxed environment.	0	11	11	44	33

The preference for VMware Workstation over AWS is re-enforced with the result:

In labs, which environment do you prefer:

Virtualised environments using stand-alone images (VMware)	[78%]
Traditional stand-alone computers with the OS and tools already prepared	[11%]
Web-based virtual environment with the interconnection of VM images	[11%]
Using AWS with a range of environments	[0%]

In terms of the things that were most successful, the students perceived that network forensics was the most successful, followed by the usage of LAMP (Linux, Apache, MySQL and PHP):

For the following virtualised labs, which was the most successful:

Network Forensics Analysis.	[67%]
Linux server configuration for LAMP.	[33%]
Authentication using ASP.NET.	[0%]
Windows 2008 server configuration for IIS.	[0%]

The main advantage of VMware is identified as its ability to be installed from home, and that it supports the study of different operating systems. A key advantage is also that the work can be sand-boxed, which is important in security and digital forensics.

Within a computing module, which is the main advantage of using VMware images:

They can be easily installed at home.	[33%]
They allow me experience of real-life virtualised infrastructures.	[22%]
They allowed me to setup a wide range of operating systems.	[22%]
They have allowed me to study remotely.	[11%]
They allow the usage of tools within a sandboxed environment.	[11%]
They supported lab setups which were already pre-prepared.	[0%]
They allowed experience of using operating system infrastructures.	[0%]
They allow an in-depth analysis of the host.	[0%]
They allow an in-depth analysis of the network activity.	[0%]

For AWS the key advantages were that it allow for experience of real-life cloud infrastructures and the opportunity to study remotely.

Within a computing module, which is the main advantage of using AWS:

They allow me experience of real-life cloud infrastructures.	[44%]
They have allowed me to study remotely.	[33%]
They supported lab setups which were already pre-prepared.	[11%]
They allowed experience of using operating system infrastructures.	[11%]
They allowed me to setup a wide range of operating systems.	[0%]

They can be easily installed at home.	[0%]
They allow the usage of tools within a sandboxed environment.	[0%]
They allow an in-depth analysis of the host.	[0%]
They allow an in-depth analysis of the network activity.	[0%]

5. Case Study 2 (Host-based Forensics)

The second case study is based on a Host-based Forensics module which runs at MSc level. This module was split into two parts: one covering the more traditional non-volatile forensics; and the second half covering the volatile forensics. The syllabus for the non-volatile forensics course covered basic investigation process, along with fundamental operating system and data theory to aid the students in understanding exactly where evidence could be found, and the challenges they would face. The students attended lectures which were then followed up by labs.

For the labs the students use a VMware configuration which was based on CAINE 2.0 (Figure 5) [5]. This is a customised Ubuntu build which integrates a number of forensics tools, including The Sleuth Kit, Autopsy Browser, regripper, along with imaging tools such as dcfldd. The labs saw the students making disk images from 'attached' drives, mounting them in the forensic environment, and using various analysis tools to extract evidence. The main difficulty with using a VMware cluster was in relating the act of attaching a drive to the virtual machine. It was not possible to attach a write blocker, and a disk had to be added to the virtual machine when it was being configured. This was as simple as 'attaching' a drive during the virtual machine configuration phase. Each of the disks could then be seen by each student once logged into the machine. However, each lab required different disk images, and keeping an up-to-date and meaningful list of disks would have aided in their conceptual analysis of how the system was configured.

The disks for each task generally came from a Windows XP Service Pack 3 desktop machine specially built for the course. This machine had a single normal user called Bernard. Bernard's profile on the machine was then used over a period of time to form a number of timelines of activities for the students to analyse in subsequent labs. One of the main activities related to building a timeline of activity around Bernard's use of peer to peer software to download images from a bit torrent service. Using evidence gleaned from the file system and registry, students were asked key questions about events along the timeline. The Windows XP disk image was converted from the Hyper-V .vhd disk format to the native WMware disk format. The disk was then uploaded to the cluster. Some points to note about this process are that it is a very space intensive operation, as each student requires their own copy of the disk. The minimum realistic (realistic enough to facilitate a form of activity) size of a Windows XP disk is about 6GB.

In addition, disk images were used that had been created by Brian Carrier as part of the forensic testing tool website. The images used in the course were FAT images that allowed students to analyse and understand the nuances involved in

4

file system and disk analysis. Of particular interest to the students was learning about tool behaviour when they were faced with a logical file system search and a logical file level search.

One of the labs required the students to make a local, forensically sound, disk image from the attached Windows XP disk. The time taken to make a disk image would double when all nine of the student instances performed the operation at the same time. Therefore, if a larger class were to perform this task, considerations should be considered to ensure that there is not a detrimental impact on the cluster.

The VMWare cluster did suffer from the fact that it took some students some time to understand the 'virtual' nature of the configuration, and some students consistently found it to be a stumbling block. This was especially true of students who were not used to a Linux environment. The issues encountered there related to conveying to them where a device was kept on the system, and the fact that it existed in the dev folder. Once mounted, additional issues were faced when students made disk images. The contact of the directory structure was sometimes not noted. The led to students believing that they had imaged a disk to their home directory when in fact it ended up in the /dev/ directory. This is a slightly more generic problem that relates to a lack of prior experience with command line environments.
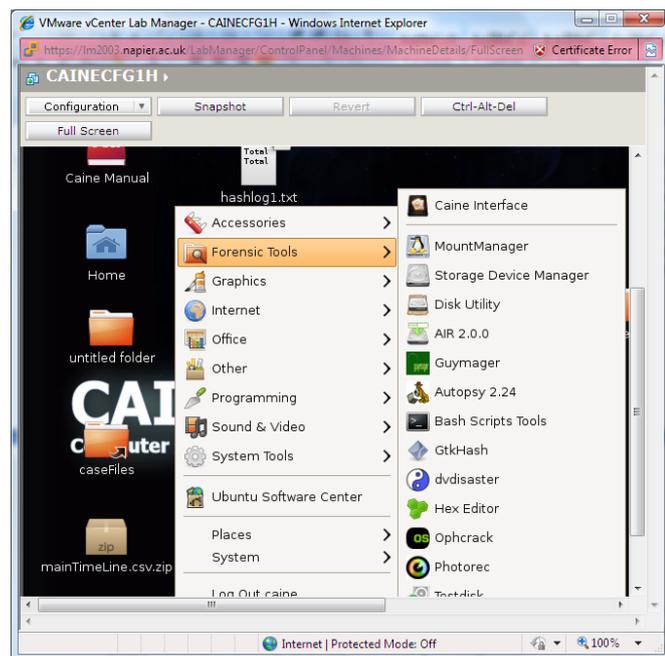
Figure 5: CAINE instance within vCenter Lab Manager

For the volatile part of the module, the VMware cluster environment was well suited to designing scenario based Live forensics labs. A secure virtualised network environment fenced from the real network was constructed using the VMware Lab Manager. VMware Lab Manager has a very intuitive management framework that reduced effort in preparing lab sessions. Fenced networks created by support DHCP, Static IP pools and Manual IP allocation that helped in configurations of labs programmatically for different live forensics scenarios. Each student was provided an ISO image of the Live Forensic (Incident Response) Toolkit, taught

during the respective lectures, which they could attach to their assigned VMs during the labs.

Metasploit [6], a malware analysis framework and penetration testing tool, was run on separate virtual machines to compromise student virtual machines and/or simulate malicious insider behaviour. The students investigated these scenarios to extract volatile information from the suspect PC and the labs were designed to focus the students on the impact of running Live Forensics tools on the suspect PC and the concept of order of volatility. For each scenario, the student was encouraged to reconsider the implications about the volatility of information. One of the scenarios used an advanced payload called Meterpreter which hides itself very efficiently on the suspect PC. Figure 6 shows the student machine on IP address 192.168.10.60 being compromised with Metrepreter payload and its shell. This lab sessions encouraged the students to understand that Live Incident response is not always sufficient to get the full context of a digital forensics incident and the "Trojan Defence" (for instance with Meterpreter) was still a possibility. This took the students to the second part of the live forensics training; Memory Analysis.
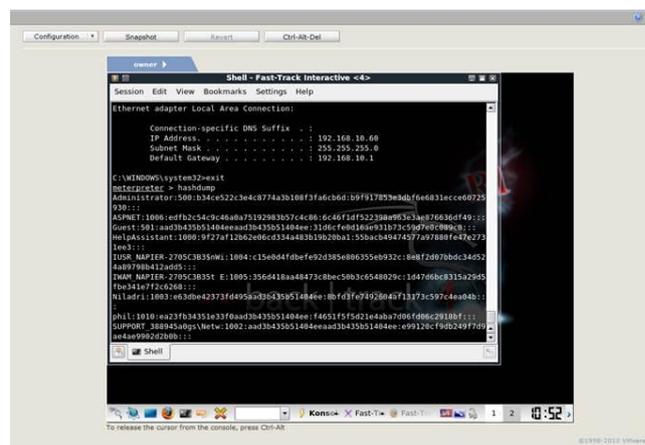

Figure 6: Metrepeter Shell Session on a virtual network

For memory analysis the students were taught various methods of extracting physical memory like hibernation files, crash dumps, Virtualisation and direct hardware access to physical memory.

On the VMware cluster the advantages of live forensic analysis in a virtual environment were demonstrated. The students created .vmem files that they produced by suspending a suspect virtual machine. The students were also introduced a free memory extraction tool called Memoryze by Mandiant Software[7] which allowed the students to extract a bit-by-bit image of the physical memory.

The students appreciated the fact that the software took in to account volatile data stored in page files. Figure 7 shows the use of Memoryze to extract memory image of a virtual machine.

The volatility framework [8] was used to analyse the various physical memory images. One of the scenarios involved detection of Zeus agent on the suspect image. The virtual image used to teach student how Zeus looks on a suspect PC was from Challenge 3 of The Honeynet Project Forensic Challenge 2010 [9]. At the end of the labs the

students were confident that they had the tools and knowledge required for memory analysis from a malware forensics perspective. As live forensics is a rapidly evolving area of research the tool installation and configurations were complex and time consuming. The VMware Lab Manager template system reduced a lab preparation and effort in creating a base images, which were configured once and then cloned for each student.
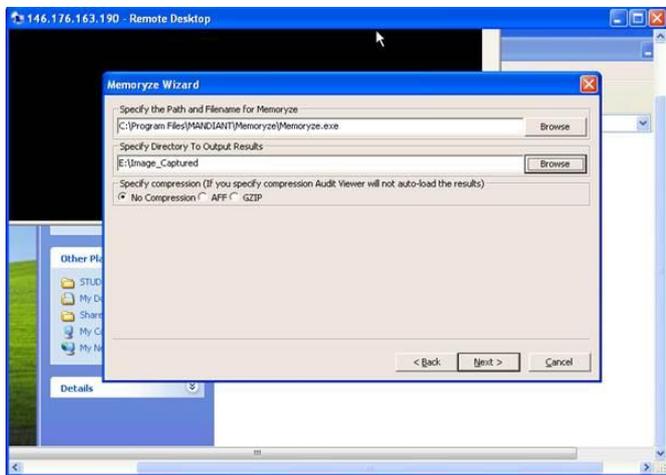

Figure 7: Memory extraction using Memoryze.

6. Case Study 3 (Security and Digital Forensics)

The third case study involves a Year 3 (BEng) level module investigating the core fundamentals of security and digital forensics, including the usage of intrusion detection systems (such as with Snort), encryption, authentication, forensic computing, network security and software security [4]. The module is assessed with two class tests, and a coursework involving an evaluation of a Web site.

In previous years the coursework was done on desktops in the lab, using Snort to detect a range of activities. For the Semester 1, 2010 session (Sept-Dec 2010) the coursework was changed so that it involved the security assessment of an online Web site which was placed within the private cloud at a given IP address. Students could then use assessment tools, such as NMAP, to discover its services, and probe for weaknesses. They then had to write Snort rules to detect certain activities. As a backup, students were also given the opportunity to use a stand-alone version of the server, so as to run it on their own PC, but most selected to do it within the private cloud.

Figure 8 shows the CPU utilization of two main ESXi hosts for the module. Overall the main cluster server coped well with four two hour lab instances per week. The second server was not needed much until the coursework, where after the hand-out date (2 Nov 2010) there was a large increase in usage, which then dropped back after the coursework submission date. This type of activity shows that students find the private cloud useful when completing coursework. The reduced usage at end of October is due to some labs being run using VMware Workstation, rather than for ESXi versions.

In terms of electrical power consumption, the cloud infrastructure has many advantages over traditional desktop, and over the semester the average power consumption has been 171W, which when considered to a lab based with 20 computers, consuming 60W each in an idle state, gives a considerable saving. Along with this, the cloud infrastructure requires only a Web interface to connect to the instances so that the computers within a lab can be fairly simple, and have minimal boot requirements (thus allowing for power savings).


Figure 8: Usage of the private cloud for Security and Forensic Computing module (Sept-Dec 2010)

7. Conclusions

The key finding of Case Study 1 is that students seem to be more engaged with the usage of virtualised environments as it allows them to work on real-life systems, while working within a sandbox. The advantages of AWS are less clear, and the main strength was seen to be gain knowledge in using a public cloud infrastructure.

Case Study 2 has shown that both Static and Live Forensics can be run successfully with a virtualised environment, including the mounting of disk images, and in analysing running machines. This provides students with, again, real-life environments on a range of operating systems (such as Windows and Linux). There were problems identified, and generally Linux instances ran much better than Windows ones, which highlights that Windows instances must be carefully manage when there are many students running them at the same time. A strong recommendation is that large classes sizes should possibly be told to stagger their boot of Windows instances, so that the system does not get overwhelmed with the initial boot up.

Case Study 2 has shown that both Static and Live Forensics can be run successfully with a virtualised environment, including the mounting of disk images, and in analysing running machines. This provides students with, again, real-life environments on a range of operating systems

(such as Windows and Linux). A strong recommendation is that large classes sizes should possibly be told to stagger their boot of Windows instances, so that the system does not get overwhelmed with the initial boot up. The lecturer should clearly explain the virtual environment and architecture to prevent confusion amongst students. The virtual environment setup described in this paper was ideal for running scenario based live and static forensic labs because of the rapid prototyping and development environment. It is possible to rapidly deploy or update images once modifications to tooling are made. It also exposed the student to live forensics practices in a Virtual or Cloud environment, which we consider the next wave of security threat.

Generally AWS is seen as useful for standardized server instances, which are pre-prepared especially for Windows 2003/2008 server environments, and for LAMP, but the usage of a range of security and digital forensic tools is probably done best within a private cloud. On observation of the developed private cloud infrastructure it is important to have at least two high powered servers are required to support modules, along with a relatively large memory capacity and a relatively large storage space for storing the VM instances. At times some of the instances took up too much resources, especially in running the CPU on the instance at near 100%, such as in kernel debug applications, and thus it is important to continually monitor instances to make sure they are not hogging too much of the resources.

The usage of virtualisation, either through a standard-alone instance (such as with VMware Workstation), though a public cloud (such as with AWS), or with a private cloud (such as with VMware ESXi) provides many advantages for teaching security and digital forensics, these include:
- Gives students full administrator privileges over the working environment
- Allows students to remotely complete labs.
- Students training on state-of-the-art infrastructures.
- Easy for teaching team to update.
- Different labs can be created for different situations (Linux/Oracle/Windows IIS/etc).
- Supports remote/distance learning.
- Helps with franchised colleges.
- Easy setup for classroom demonstrations.
- Infrastructure can be ring-fenced.
- Supports group work in an isolated environment.
- In-depth analysis of infrastructures.
- Students can build systems from scratch.
- Students can update their own infrastructure/tools, as required.
- Produces repeatable labs.
- Not dependent on network infrastructure.
- Seems to engage the students, and show them a wide potential.
- Encourages students to continue work after the lab/tutorial.
- Time windows of labs/tutorials can be carefully controlled.

But there are disadvantages including:

- Requires an investment in time in creating and maintaining the virtual image.
- Students can avoid the lab situation.
- Possibly requires a backup strategy for labs (if using network-based virtualisation – but has advantages that a standalone version does not need a network connection).
- Goes against the stand-alone machine philosophy.
- Raises issues related to software licensing and network security.

Overall the key focus is that the usage of virtualization is likely enhance the employability of students, as they can work on a range of environments, and with real-life scenarios. A common comment from law enforcement professionals is that students often are well equipped from an academic point-of-view, but struggle to show any real hands-on experience. With virtualization, the infrastructures can be setup so that students can gain this experience, no matter if there are in a physical lab, or working remotely. VMware ESXi has proved to be an excellence teaching environment, as it can be easily configured to support fairly large class sizes.

ACKNOWLEDGEMENT

REFERENCES

[1]   VMware Academic Program, http://www.vmware.com/partners/academic.
[2]   Hping reference, http://www.thefullwiki.org/Hping
[3]   Security and Forensic Computing module, http://www.soc.napier.ac.uk/~bill/index_sfc_napier.html
[4]   Advanced Security and Digital Computing module, http://www.dcs.napier.ac.uk/~bill/index_asfc_napier.html
[5]   CAINE 2.0 (Computer Aided Investigation Environment), http://www.caine-live.net/.
[6]   Metasploit http://www.metasploit.com/
[7]   Memoryze http://www.mandiant.com/products/free_software/memoryze/
[8]   Volatility Framework https://www.volatilesystems.com/default/volatility
[9]   Honeynet http://www.honeynet.org/challenges/2010_3_banking_troubles
[10]   Buchanan, W., Macfarlane, R., Ludwiniak, R., Student Perception of On-Line Lectures with a Blended Learning Environment, The 4th International Conference on Cybercrime Forensics Education & Training, Canterbury.

*The following diagrams have been added for clarity.*

Private Cloud – owned and run by an organisation

Community Cloud – shared by several organisation, with a common policy, compliance, mission, etc

Public Cloud – owned by an organisation selling a cloud infrastructure

Hybrid Cloud – two or more clouds

Figure 1: Cloud infrastructures

Client

Windows	Local Virtualised (eg VMWare Workstation)
OS	
NAT (Network Address Translation)	

OS and Services can be either temporal or permanent (until deleted)

	Services
Windows	Lunix		Other OS
VMWare ESX (bare metal virtualisation)			

OS		Services
Remote Virtualised (eg WMWare Workstation)		
Base OS		

Server cluster

Figure 2: VM instances

VMWare Workstation/ Fusion

VMware vCenter

Amazon Web Services

**Figure 3:** Alternatives

Figure 4: VMWare ESXi infrastructure
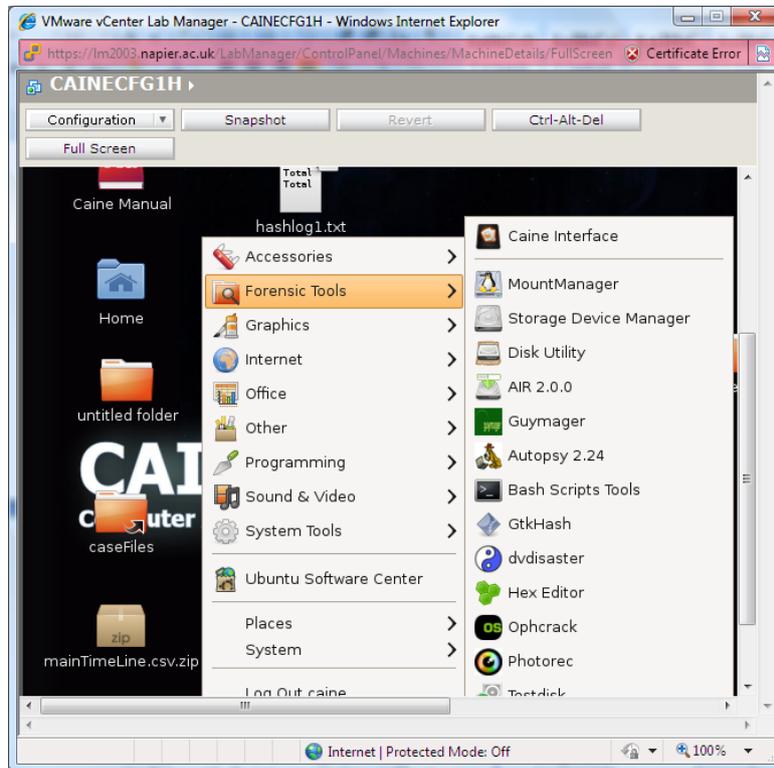
Figure 5: CAINE instance within vCenter Lab Manager
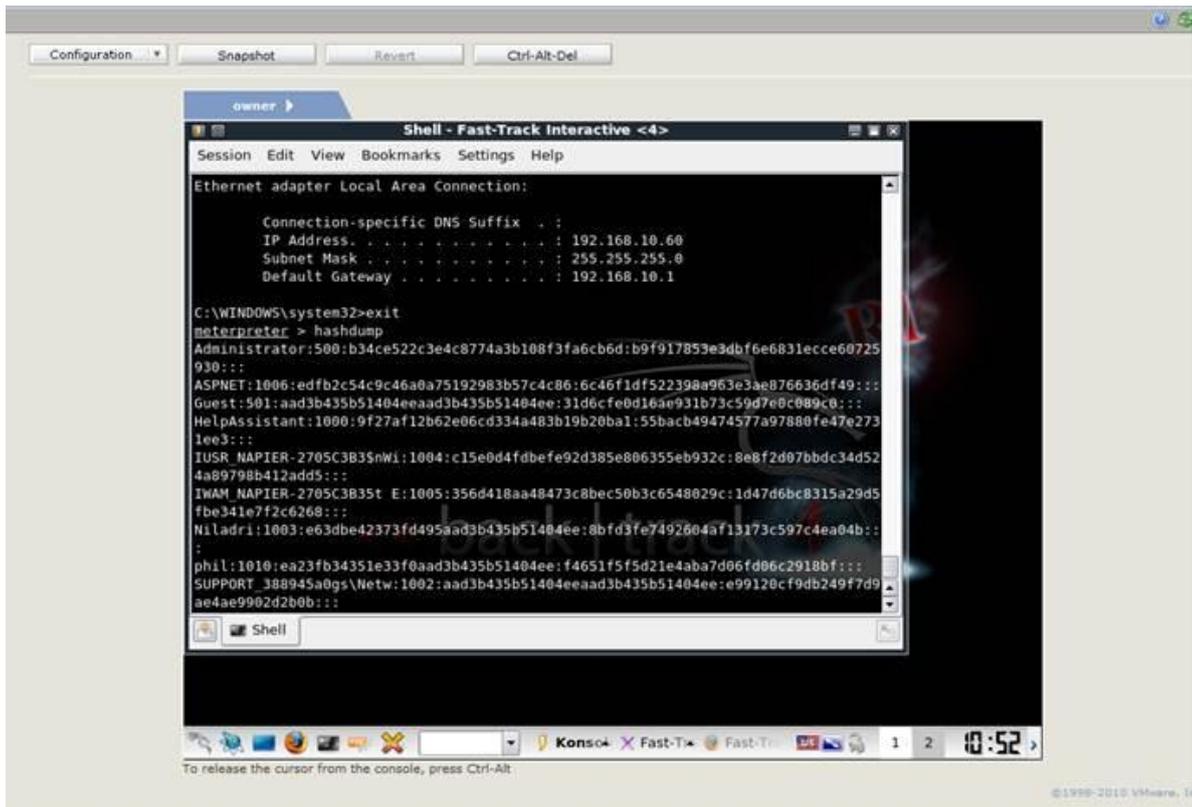
Figure 6: Metrepeter Shell Session on a virtual network
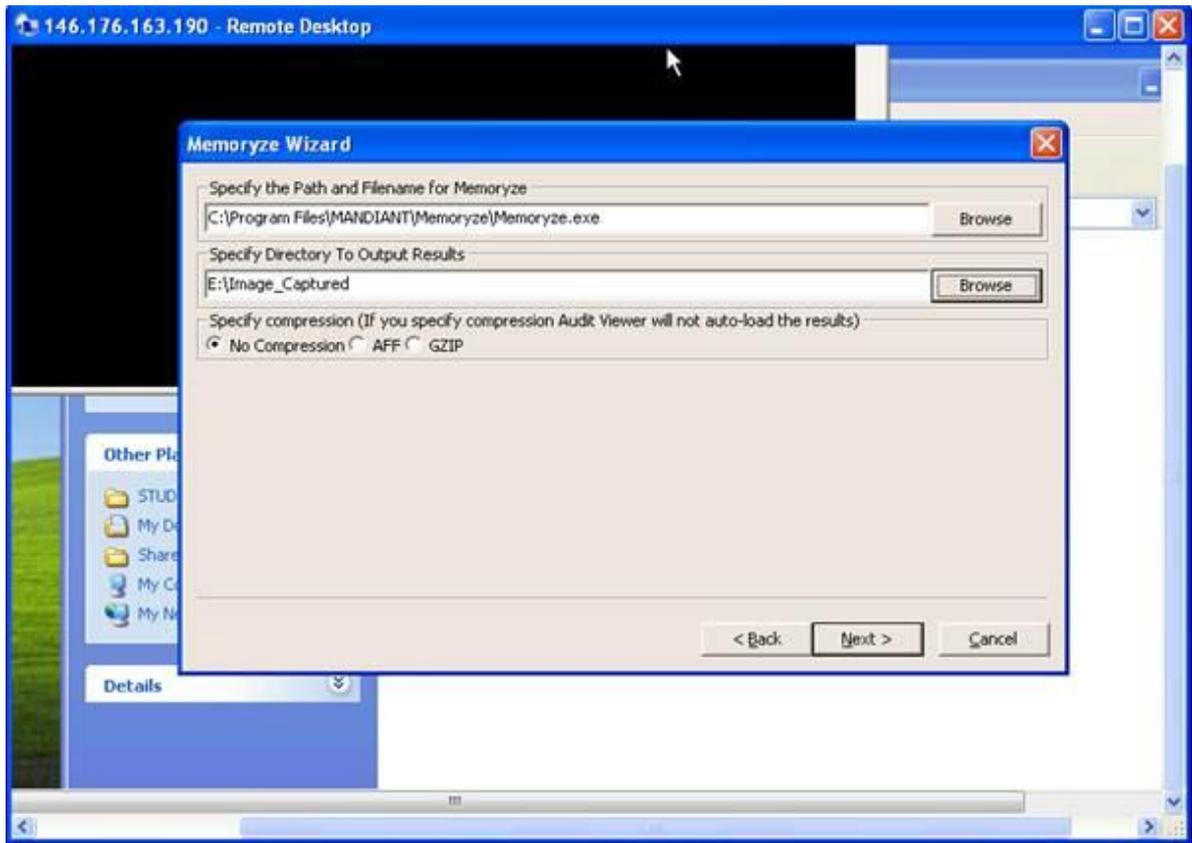
Figure 7: Memory extraction using Memoryze.
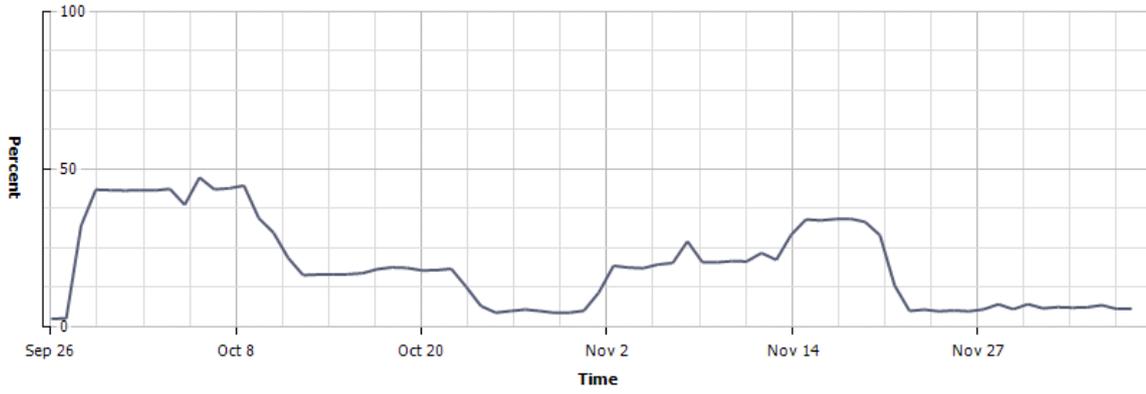
CPU/Custom..., 25/09/2010 11:24:26 - 09/12/2010 11:23:10 Chart Options... Switch to:

Performance Chart Legend

Key	Object	Measurement	Rollup	Units	Latest	Maximum	Minimum	Average
■	146.176.166.65	Usage	Average	Percent	5.29	47.18	2.14	19.204
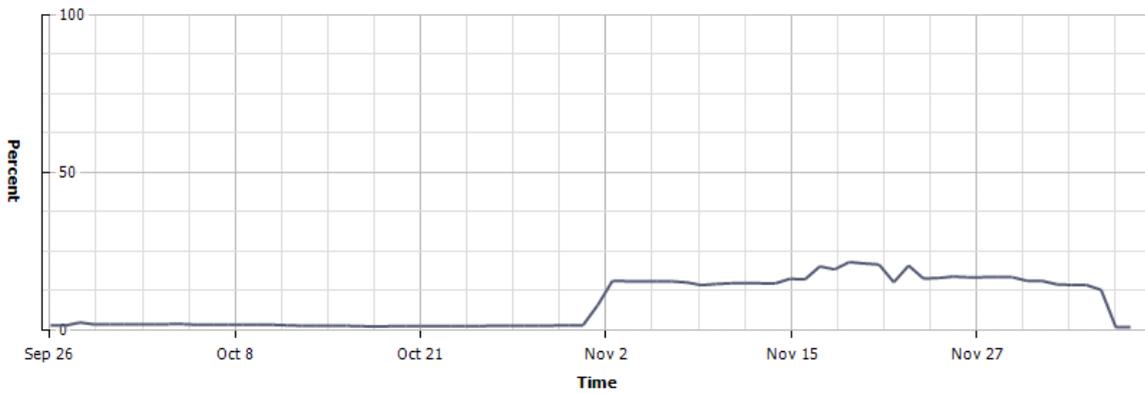
CPU/Custom..., 25/09/2010 11:26:59 - 09/12/2010 11:26:59 Chart Options... Switch to:

Performance Chart Legend

Key	Object	Measurement	Rollup	Units	Latest	Maximum	Minimum	Average
■	146.176.166.69	Usage	Average	Percent	0.49	21.28	0.48	8.041

Figure 8: Usage of the private cloud for Security and Forensic Computing module (Sept-Dec 2010)