The All Round Cyber Crime and Security Professional: Circular Teaching for the Professional and the Technical – Experiences from the Witness Box

Abstract

In the ongoing battle against cybercrime, digital forensics is an increasingly important branch of cyber security, in an ever changing field of study where professionals and students alike need to learn and dissect key skills in order to stay at the cutting edge of their professions. This paper incorporates techniques, ideas and the progress made on our University Digital Forensics Module. In this module students were empowered through learning hard and soft skills that enabled them to develop and play out the role of an expert witness in a real world court room scenario. Details in terms of court proceedings, crime scene set up, statistics and feedback are included.

Techniques employed in this module included live RAM (Random Access Memory) capture, internet history analysis, data carving and evidence handling. Once students had developed these skills, they prepared an in-depth witness statement detailing their involvement in the case. This was accompanied by a digital forensics report that set out how the evidence gathered is relevant to the case.

Keywords

Cyber Security, Cybercrime, Digital Forensics, Learning, Teaching, RAM Capture, Crime Scene, Court, Law, Open Source

Adrian Winckles (adrian.winckles@anglia.ac.uk) and Andrew Moore (andrew.moore@anglia.ac.uk)
Faculty of Science and Technology
Introduction

In these challenging times of increasing data and security breaches, our cyber security professionals require hard technical skills. To meet the rapidly increasing complexity of cyber conflict this must be combined with the softer but no less essential skills of forensically sound data recovery (Lessing & Von Solms, 2008), the ability to summarise the data in layman’s terms, and the ability to withstand the scrutiny that their findings will be subjected to in various legal contexts.

On our Security and Forensic courses we have developed a successful combination of these hard and soft skills. Forensic and IT Security students were provided with a relevant crime scene scenario including live memory capture and seizure of digital evidence. This involved both promoting discussion on contamination of evidence, such as the Association of Chief Police Officers (ACPO) / National Institute of Standards and Technology (NIST) digital evidence guidelines, and conventional evidence gathering (Reith et al., 2002) at the custom built crime scene.

In addition, students were prepared for forensic handling and analysing of the evidence with specific emphasis on report writing and summarisation skills. The ultimate goal was for the students to write an independent witness evidence report based on the forensic analysis of the evidence found. The final challenge for the students was a court appearance as an expert witness, where their expert witness report had to be justified and stand up to scrutiny under cross examination by both the prosecution and defence.

An authentic court room experience was achieved by using a combination of retired judges, retired magistrates, ex-police officers and current law students. Students reinforced the success of this approach by reflecting on the experience this module brings to a well-rounded cyber professional.

Objectives and Learning Outcomes

To provide a student with a comprehensive learning experience the following objectives needed to be met:

- Authentic court room and crime scene simulations to provide a professional, real world feel
- The use of professionals with real court room expertise
- The use of forensically sound tools (open source and corporate) to ensure that forensic examination could be carried out and verified
- The briefing of students on the Chain of Custody to enable them to demonstrate in court that evidence handling procedures have been followed
- The briefing of students that they are trainee digital forensic experts and should only comment on evidence pertaining to their area of expertise
- To ensure that during the court scenario the students are cross examined by a defence and prosecution who have a wide variety of experiences in law
- To ensure compliance with University ethics and health and safely policies
- To ensure that the module would be marked fairly and without bias

Curriculum and Learning

The curriculum was based on a combination of ACPO/NIST guidelines and higher level learning modules (Craiger et al., 2007). The module spanned 12 weeks during which students learnt the various methods and approaches to follow when it came to seizing and handling evidence from a potential crime scene. The module was split into two parts. During Weeks 1-6 students prepared for seizing evidence and acquiring it scientifically. Once the students had acquired and transported their evidence from the simulated crime scene, the remaining weeks gave them time to analyse the hardware and to find the evidence. Students then had to present the evidence in court in a professional format, clearly highlighting the scientific evidence but also presenting it in such a way that laymen, such as a jury, could grasp. The court scenario required them to submit an evidence report, a witness statement of evidence found and where they had found it.
Breakdown of Curriculum (Weeks 1-6)

Table 1 contains the module content and work schedule for lectures and workshops for weeks 1-6 on the module, Digital Forensics.

<table>
<thead>
<tr>
<th>Week</th>
<th>Lecture</th>
<th>Seminar / Workshop</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction to the module, touching on Crime Scene procedures and management</td>
<td>Case study brief and software demo</td>
</tr>
<tr>
<td>2</td>
<td>Identification and Seizure – Identifying, Seizing and storing Electronic Evidence</td>
<td>Evidence handling</td>
</tr>
<tr>
<td>3</td>
<td>Live Capture techniques of exporting RAM</td>
<td>Crime scene recovery – RAM</td>
</tr>
<tr>
<td>4</td>
<td>Recovering Internet History and emails</td>
<td>Crime scene recovery – Emails and internet history</td>
</tr>
<tr>
<td>5</td>
<td>Recovering Forensic Artefacts</td>
<td>Windows Registry / previously installed files and programs</td>
</tr>
<tr>
<td>6</td>
<td>Crime scene brief and theory</td>
<td>Crime scene practical activity</td>
</tr>
</tbody>
</table>

Table 1: Digital Forensics module content – Weeks 1-6

Learning Breakdown (Pre-Crime Scene)

Each week students attended a lecture followed by a practical lab session later in the day. In the first week, students were given an introduction to how the module was to be taught and what was expected of them. This was followed by a lab session, in which they covered laboratory setups, and learnt how to use forensic software (Encase v7) efficiently.

The following week covered how evidence is acquired, handled and transported without contaminating either it or the crime scene (Ieong, 2006). The practical session involved demonstrations of protective suits, doubled-up gloves, and equipment to provide students with the best possible experience while complying with University ethics and health and safety procedures.

Live RAM (Random Access Memory) capture was then demonstrated using a variety of tools ranging from open source command line, text-based tools, to the more professional tools with GUIs and moderate ease of use built in. The aim was to highlight to students that not all professional tools return the same answers in terms of spotting anti forensics techniques or malware infections. This was demonstrated by asking the students to complete a series of steps with different sets of tools using both clean and botnet infected RAM images.

The student then translated information such as currently- and previously connected devices and their Internet Protocol (IP) addresses into an easy-to-read format. This was to ascertain if the IP addresses had been hacked, infected or altered in any way, ensuring the student understood the requirement to present the evidence in a way that less technical people could understand the importance of each point (Müller & Spreitzenbarth, 2013).

The next section taught students how to recover deleted emails, internet browser history, and previously installed programs from the suspect machine. The students tried a combination of open source and professional tools to identify which gave the best results (Carrier, 2002). During this exercise, programs such as TrueCrypt were found on the computer (TrueCrypt allows the user to create ‘container files’ that can hide data in plain sight). This was revisited in Week 8 (see below) when the students were shown how to find TrueCrypt container files, which have a ‘.tcy’ extension, which may contain hidden data linked to the case.

Jargon Buster

**Open Source:** ‘a computer program in which the source code is available to the general public for use and/or modification from its original design’ (Wikipedia)

**Command line:** ‘a means of interacting with a computer program where the user (or client) issues commands to the program in the form of successive lines of text (command lines)’ (Wikipedia)

**Graphical User Interface (GUI):** ‘a type of interface that allows users to interact with electronic devices through graphical icons and visual indicators’ (Wikipedia)

**Botnet:** ‘A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks… The term is usually used with a negative or malicious connotation’ (Wikipedia)
Learning Breakdown (Crime Scene)

Once they had learnt basic evidence handling and processing procedures, students were required to complete the first stage of the module by undertaking a practical crime scene activity in Week 6 (the mid-point in the module). The crime scene was set up in one of the forensic science labs at Anglia Ruskin and resembled a one-bedroom home.

Diagram 1: Crime Scene layout

In pairs, the students entered through Door A and moved into a narrow hallway. The students changed into their forensic suits, doubled-up gloves, and boots, and were given evidence bags, their choice of software, and were briefed that this process complied with the ACPO guidelines (Williams, 2012). The scenario was that a potential drug deal had gone wrong and the police had called in a digital forensic expert to acquire any evidence that could be linked to the drugs or any drug-related offences. The crime scene had already been swept by the forensic science investigators so now it was their turn. The students worked in pairs to enable one person to complete the logbook with dates, times and notes, while the other student photographed the evidence using a digital SLR camera. The images were given to each group once the activity was complete.

The students were required to seize anything they believed could potentially be digital evidence, such as a device that could hold a digital signature (Cox et al., 2007). These devices could range from a memory stick, a PC hard drive, or a camera. To add an extra degree of difficulty, substances that resembled drugs were present at the crime scene as well as stale blood stains. One of the key objectives for the students was to show that they were in the role of a digital forensics expert, not that of a forensic scientist. Commenting in their statements that drugs were present at the scene would damage their credibility in court as this is not their field of expertise (Sprowl & Sprowl, 1976).

The students entered the crime scene through Door B and began their sweep of the room. Students normally swept the crime scene in a clockwise direction to limit the risk of missing key evidence. The students were monitored from the CCTV Room (see Diagram 1). This allowed them to be assessed from a distance safely without any interruptions. Most students noticed a running PC on top of a table. They were asked to photograph any potential evidence before they touched it so they could prove it came from the crime scene. Students learnt in Week 8 that TrueCrypt passwords are stored in RAM and, as this is lost when the PC is switched off, they must perform a live memory dump to capture the data. Once they had done this they powered off the PC and bagged and tagged it as evidence.

A similar procedure was followed for acquiring evidence from already powered off/unplugged equipment. As before the objects were photographed, carefully placed in an evidence bag, and tagged accordingly (Bulbul et al., 2013). Once the students had collected the evidence, they safely transported it to a locked container. Once they had completed this activity, the students returned to the crime scene to receive their photos and feedback. The objects were then repositioned in the crime scene and the PC powered on, ready for the next group.
Breakdown of Curriculum (Weeks 7-12)

Table 2 contains the student curriculum guidelines and work schedule for lectures and workshops for Weeks 7-12.

<table>
<thead>
<tr>
<th>Week</th>
<th>Lecture</th>
<th>Seminar / Workshop</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>How to write a forensic statement</td>
<td>Forensic statement scrutiny</td>
</tr>
<tr>
<td>8</td>
<td>Removal and recovery of encryption and hidden layers</td>
<td>Forensic Investigation</td>
</tr>
<tr>
<td>9</td>
<td>Forensic Data Wiping – SSD and HDD recover methods</td>
<td>Forensic Investigation</td>
</tr>
<tr>
<td>10</td>
<td>Court Room case brief and theory</td>
<td>Presentation of work in court</td>
</tr>
<tr>
<td>11</td>
<td>Reflective essay writing</td>
<td>Court room feedback; dos and don’ts</td>
</tr>
<tr>
<td>12</td>
<td>Summary of technical skills learned and theory of future forensic concepts</td>
<td>Report writing and catch up week – (overflow)</td>
</tr>
</tbody>
</table>

Table 2: Digital forensic student curriculum Weeks 7-12

Learning Breakdown (Court Room Preparation)

Having completed the crime scene activity the students spent the remaining weeks preparing for the court room scenario. Week 7 started with a tutorial on how to write an expert witness report. Students were given the template used by Cambridgeshire Constabulary and other law enforcement agencies (Bates, 2013). The students were also given a guest lecture on statement writing and court room etiquette by a lecturer from the Law department at Anglia Ruskin. Students also revised what they learnt in Week 1 as they were required to provide an *Encase* report with their witness statement to detail the breakdown of potential digital evidence found.

In Week 8 the students learnt how to the find *TrueCrypt* files using open source software. As noted above, *TrueCrypt* is encryption software that allows the user to hide their data in plain sight, cloaked as another file. Students were taught how to locate the hidden *TrueCrypt* file using software tools such as *TC-Hunt* and *TC-Head*. Once they had found the file, the student completed their RAM analysis to extract the container’s password from the running memory (Miao, 2010). The password was then used to open the suspect’s *TrueCrypt* file, thus enabling the student to present more robust evidence for the case in court. As described above, students had taken a memory dump of the RAM on the suspect’s PC. They were able to extract the *TrueCrypt* password from this and use it to open the encrypted file.

Once the students had analysed the data and completed the necessary documents, they had to present their evidence in court (Casey, 2011). The court room set-up and floor plan is shown in Diagram 2. The judge was played by a retired judge, and the defence and prosecution were played by a combination of Anglia Ruskin Law students and professionals who volunteered their time to this module. The jury box contained the student assessor, who, as well as the judge, took notes of each case.

The student entered through Door A and took the expert witness stand. The student then gave the Promissory Affirmation: ‘I do solemnly, sincerely and truly declare and affirm that the evidence I shall give shall be the truth the whole truth and nothing but the truth’. This secular option was chosen as it meets with the University’s ethics policy and does not require anyone to openly state their religious beliefs. Each session ran for approximately 30 minutes although extra time was built into the scheduled timetable if required. The court room scenario was divided into four sections. Firstly the judge asked the prosecution to begin their open arguments, asked the expert witness to read their statement, and passed proceedings over to the defence. The defence then asked set questions which were a combination of standard scenario questions and three tough technical questions aimed at ascertaining how strong the primary evidence work was. The defence was also given the opportunity to ask questions of their own choosing in the final minutes of each session.

**Jargon Buster**

**SSD:** ‘A solid-state drive… (though it contains no actual disk) is a data storage device [which has] no moving (mechanical) components’ (Wikipedia)

**HDD:** ‘A hard disk drive… is a data storage device used for storing and retrieving digital information using rapidly rotating disks (platters) coated with magnetic material’ (Wikipedia)
Once the defence had completed their cross examination, the prosecution was allowed to ask a few more questions. Finally the judge and assessor had the opportunity to ask the student questions, and, when all questioning was finished, the session closed.

Statistics and Feedback

At the end of the module, students completed feedback forms, which included a free-text comments section. The form asked students to describe their experience of the various elements of the module (e.g. the live capture, court room, and crime scene components) and to note any difficulties they had experienced during the module.

Module Statistics

The module Digital Forensics consisted of 24 second-year students. Feedback was based on 12 questions each scoring a maximum of 5 marks. The percentages for Overall Satisfaction range from 63.3% to 95.0% with a mean rating 84.1%. If the response from student one (outlier—10.4% lower than the next highest mark) is removed from the calculation, the average score increases to 85.0%. This is a 4% increase, which highlights the further potential for an increase in satisfaction with the next delivery of the module.

Feedback Breakdown and Details

<table>
<thead>
<tr>
<th>Question</th>
<th>Statistics</th>
<th>Feedback received</th>
<th>Action as result of feedback (if required)</th>
</tr>
</thead>
</table>
| Did the Live Capture Demonstrator, Crime Scene and Courtroom have a positive experience? | 76% positive feedback | ‘RAM capture very realistic’  
‘Very positive, the judge was brilliant’  
‘Was a very good experience but could have been harder in the crime scene’ | Next delivery the RAM analysis may stay but made harder however new technologies such as Apple based devices or Mobile will be introduced in line with the rest of their degree. |
| Did this have any major benefits?                                       | 72% positive feedback | ‘got the experience of a real life court case’  
‘experience of crime scene and court’ | Feedback is slightly lower in this area. The benefits will be better clarified next time around. Possibly an external speaker could show the students how this module could benefit them. |
| Have you experienced any difficulties? How have they impacted your learning experience? | 83% positive feedback | ‘No’  
‘linking the witness and encase reports together was difficult at times’ | Witness statements writing will cover more on the link between the statement and the technical report, not just building the documents. |
The All Round Cyber Crime and Security Professional: Circular Teaching for the Professional and the Technical – Experiences from the Witness Box

### Table 3: Statistics and feedback

<table>
<thead>
<tr>
<th>Question</th>
<th>Statistics</th>
<th>Feedback received</th>
<th>Action as result of feedback (if required)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Would you change anything?</td>
<td>77% positive feedback</td>
<td>‘longer time gathering evidence’ ‘different scenario to drugs’</td>
<td>Next delivery will offer a new scenario. The crime scene will be streamlined to ensure the time is used more efficiently.</td>
</tr>
<tr>
<td>Support and feedback from instructor and support staff</td>
<td>79% positive feedback</td>
<td>‘support was good, VLE content need updated quicker’ ‘instructor was very passionate in what he taught’</td>
<td>Feedback was good and the VLE (virtual learning environment) will be monitored closely.</td>
</tr>
<tr>
<td>Was the judge debriefing useful?</td>
<td>84% positive feedback</td>
<td>‘Feedback was somewhat harsh but helpful ‘helped me out a lot due to his honesty’</td>
<td>Feedback seemed positively high. Next time more than one professional source outside the university could give feedback. Such as a currently serving police officer</td>
</tr>
</tbody>
</table>

### Conclusion

This paper has demonstrated that using the correct course curriculum, real world factors and technology, a real world experience can be achieved. The tools used in the module included both open source and commercial forensic software, these highlighted to students how learning objectives can be achieved professionally and efficiently. The students gave feedback that will be used to improve the next delivery of the module. Highlights for the students were the build-up to, and the actual day of the practical sessions, in which students presented evidence they had acquired to the court in a professional manner.

As a whole the feedback was positive and highlighted areas where improvement could be made to deliver a stronger real world experience. The professionals and the collaboration from the Anglia Ruskin Law Department demonstrated that a high standard can be achieved.

### References


