Digital Forensics Masterclass

Reflective Report

Fraser Brown

Software Engineering MEng

H00155918

Contents

1 Producing Lab & Lecture Materials

This master class has allowed me to investigate and learn about a field within computer security I was passionate about - Digital Forensics. Digital forensics was going to be one of the areas I researched in my spare time, the fact I could do this and have it count towards my degree was great. I enjoyed the learning process, and research: reading articles, papers, books, and doing practical learning in this field etc. I felt I was able to transfer my enthusiasm into the lecture and lab materials, which was great.

More importantly having a module centred around producing teaching materials was really interesting as it challenged the way in which I learned about my topic. My main concern was not if I understood something well enough to do the practical lab, but was now focused on if I understood the topic well enough explain it to others. This was a really interesting perspective I had not experienced before, and I honestly loved it. Being able to refine my explanations and materials to teach things I personally found interesting was a lot of fun. It pushed me to delve deeper into certain areas of file system forensics to make sure I was explaining the area correctly and more importantly in the most engaging way possible.

I thoroughly enjoyed the whole process from creating learning materials to giving the lecture and lab, it was one of the most rewarding courses I've taken in my 5 years at university. Being able to see that same excitement and "eureka" moments on attendees faces which I had felt myself just weeks ago was very rewarding. Not only did it display their interest in the content but it meant I had explained the topic well. I would highly recommend this module to others and to use this method of learning in coursework going forward.

2 Lecture

Overall delivering the lecture went really well. I had never spoken to a large number of people for and hour before and was rather nervous about it. However despite this I felt like I was able to get into a flow after the first few slides, the nerves faded slightly and I was able to enjoy the lecture. It felt like I was talking about a field I was interested in for an hour, rather than an assessment for coursework.

Rather than just give a lecture my plan was to create a good learning environment, this would allow me to set the scene and help get the audience in the mood for the material they were about to sit through. As a result I dressed up the room like a crime scene with “crime scene do not cross” banners, my aim for this was to help the room relax and break the ice. It was received very well from all attendees, which was nice.

2.1 Areas I am Proud of

There were many areas of the lecture that I feel went well and I would consider them proud moments. I feel I was able to present in a casual but informative style, adding in humour and class participation throughout. This was a general aspect of my presenting I wanted to improve and felt I did this during the lecture.

Digital forensics was a new field to many members of the audience, and although it was rooted in computer science (CS) concepts, there was more to digital forensics than just the CS technical knowledge. Areas like forensic process and its connection to legal aspects were just as important and received well. I am proud of the way the audience followed along with my lecture structure and feel it helped solidify the learning.

I was able to talk about background and other related information and did not just read off the slides, this proved to me my solid understanding of the subject area, and was noted by those that attended. In addition I was able to further explain complex elements using a whiteboard and a practical example, doing so really appeared to help the audience members grasp the low level file system concepts I was describing.

I am very happy with how I answered questions at the end of the lecture it became more of a discussion about the field which was fun.

I am really proud of how well the scenario and practical examples were received in the lecture. It was a concern of mine that showing terminal output would put people off however felt it was necessary to help them understand the accompanying lab. When walking through the practical example I was able to call back to previous theory points I had mentioned from earlier slides showing how they relate. This resulted in essentially going through a forensic investigation and its stages with the audience. This went really well and paid dividends in the lab.

I'm happy with the use of diagrams and how they aided me in explaining complex areas of file systems, it allowed me to explain pointers and give a more visual element to descriptions. They were widely received well.

I am happy with how I recovered from a stumble midway through. My mind briefly went blank while explaining an area, I took a second, gathered my thoughts and continued. I knew this kind of event in a presentation previously would have set me off my stride however I am extremely proud of how I managed to recover.

I feel that my learning objectives for the class were met. After reading the peer reviews and talking to the attendees, they seemed to all come away with one or more of my learning objectives clear and understood which was amazing.

Most of all however I am extremely happy that I have been able to peak interest into the field for others that were not as aware of it.

2.2 Areas of Improvement

There were various areas I felt I should improve in. I was really nervous to start with and felt that I was talking fast. I need to remember to slow down in the future and control that, as it meant the start of the lecture may have seemed rushed as I was trying to find my feet.

I feel that I could have stopped and queried how the room was doing more often. For instance stopping at diagram slides longer to help people digest the information better.

There was a point where I stumbled (discussed above), and I believe if I made prompt cards containing reminders for difficult areas found during practice runs, this would have been less of an issue.

I would liked to have added a case study to the lecture this would have nicely rounded off certain areas and tied my topic back to the real world. This will be something I add in future lectures.

2.3 Review of Feedback Received

There was a lot of positive feedback which I am extremely happy about I will give a brief overview of some of it. For instance some enjoyed the wide range of tools that I showed and liked that there was not just a focus on one. Others praised the structure of content and stated that they enjoyed hearing the depth in background knowledge when discussing certain points.

In addition there was a strong appreciation for the tool examples and early exposure before going into the lab. Not only because it made the transition smoother but that it solidified the concepts discussed in the lecture.

2.4 Constructive Feedback Received

I got some constructive feedback from the audience which was great I will give some examples. For instance some attendees mentioned that I "spoke quite fast" at some points due to nerves and that I should consider slowing down, especially if the audience members were not all native English speakers. This is a great point and a perspective on the speaking fast element I did not originally think of. It will be something I look to improve in the future.

Another example of constructive feedback was a request for more information about other "hardware that can be investigated" - as the lecture only focused on USB media investigation. This was a great point and something I wish I had touched on, It is definitely an aspect I will add when giving the presentation in the future. It picked up on an important learning point of more concrete examples to solidify the concepts.

3 Lab

This lab was everything I wanted it to be, there were moments where I could see people really understanding the concepts they had heard about in the lecture. Genuine excitement was visible when participants were locating evidence and recovering files manually, it was great to see.

I knew when creating the lab materials that this would be unlike any other lab we have done before at university. Instead of a programming focused lab where we would build a product, this lab would push attendees to apply their CS knowledge in a different way - using it to locate hidden information. I also wanted the lab to be grounded in a scenario that would occur in the real world to give context to the tasks. Furthermore since this lab would be potentially new ground for many of the attendees, I wanted their to be a method for the participants to gauge their progress.

As a result the lab was framed around each participant being part of a hypothetical forensic investigation team, that was attempting to prove or disprove if an individual had leaked sensitive information from a company. The method of gauging progress was done with a capture the flag (CTF) style element. Where each task had some result they would have to enter into a script file, the script file would then confirm or deny if that was correct. This would allow users to gauge how they were doing and if they had found the right evidence to help the client. Both the scenario and the CTF elements were received well by those that took the lab, which I was pleased about.

3.1 Areas I am Proud Of

There were not a lot of questions about the lab material or tasks other than command syntax questions. Participants seemed to understand what was being asked of them and were able to follow the lab materials well. In review forms and discussions with attendees after the lab, many told me that the lab was clear and easy to follow which was great.

Many attendees said that the content in my lecture made the lab easier to understand I am very happy with this level of synergy between the lecture and lab materials.

I am extreemly happy about the continued attendance of my lab, in other peoples master classes I seen attendees leave after an hour, but all those that attended mine stayed for the 2 hours. Everyone seemed interested in the tasks which was great to see. Another thing that I am proud of is the ability for participants to complete the lab in the time frame (2 hours) this showed me that I had anticipated both the difficulty and completable workload in the time frame well.

3.2 Areas of Improvement

So the main bottle neck and trouble points of the lab were in the set up of the virtual environment. I knew this would be a problem and attempted to make it as smooth as possible with ample additional resources and pre set-up communications with the managers of the lab. However despite this certain participants were struggling getting an environment set up. This was not a problem with the materials I had produced it was more an unavoidable issue with the PC's themselves. I felt this took away slightly from some of the participants experience during the lab but it sadly was one of those things that could not have been avoided. In order to try and circumvent this issue in the future, I would like to contact each potentially attending person beforehand with set up requirements and have a more open dialogue with the lab maintainers to make these issues not appear in the future.

During the lab there were two things I did not anticipate: one, the set up of a virtual machine having errors relating to USB drivers. As the lab was no longer using physical USB drives to generate forensic images (another method was used), I forgot to mention that switching to the 1.1 USB drivers was required within virutalbox. This lead to some set-up questions. Adding it to the lab materials would have streamlined the process. Two, I forgot to add that the participants would have to install libreoffice on the virtual machine, this was a package that was installed on my testing environment from previous unrelated work I was doing and I assumed it came pre installed with Kali Linux this was an over sight on my part.