I really enjoyed this last class. I think the cyber security class was more informative than spatial data and the 'joy of queueing' class. I have always liked cyber security and hacking in general. I even tried to learn some basic things using an app called Mimo, but this lecture gave me way more insights about cybersecurity than an entire course in Mimo.

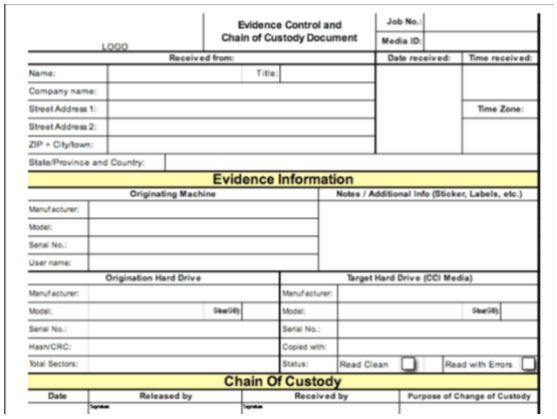
As I was saying I learned a lot of things from this lecture. One thing that I knew was the fact that data will not be completely deleted when it is deleted on the GUI of the computer. But what didn't know was that it could be replaced with other files to completely destroy the evidence. This sounded so new and eye opening to me.

We also talked a little bit about the rules that are in place for cyber security. One thing that was very interesting to me was the fact that all computer and phones are encrypted these days. Another thing that was striking to me was the fact that police or the persons of authority can force you to open your phone and you can refuse by saying that you have "forgotten" your password and you can get away with major crimes. I think the Irish authorities have to force big corporations to decrypt the evidence in case of a major crime. This would significantly decrease cybercrimes.

The lecturer also told us an amusing story about a bullet-proof hosting service. I was really impressed with the way that the host of this service got away with all the charges facing him. What he did was that he placed some magnetic fields in the door frame and when the police took the servers as evidence all of the data disappeared.

Another eye-opening thing that we learned was that the police gets a copy of the hard drive and carries investigations on that cope(image). I think it was very intriguing that the police will wipe out the forensic image's hard drive 7 times after they are done with it. Another compelling thing was that they take a Forensic Imaging rather than taking a backup, because backups do not necessarily take all the files and from the drive like files that are corrupted or partially overwritten.

We also learned about chain of custody.
Some of the details that should be provided by the person who carries the device ,according to ACPO guidelines, are shown in the image. I think it is important for us to learn these rules now so that we can have an easier time if we choose this path.



Evidence Control and Chain of Custody Document

LOGO

Job No.:
Media ID:

Received from:

Name: Title:
Company name:
Street Address 1:
Street Address 2:
ZIP + City/town:
State/Province and Country:

Date received:
Time received:
Time Zone:

Evidence Information

Originating Machine
Manufacturer:
Model:
Serial No.:
User name:

Notes / Additional Info (Sticker, Labels, etc.)

Origination Hard Drive
Manufacturer:
Model:
Serial No.:
Hash/CRC:
Total Sectors:

Target Hard Drive (CD Media)
Manufacturer:
Model:
Serial No.:
Copied with:
Status: Read Clean Read with Errors

Chain Of Custody

Date	Released by	Received by	Purpose of Change of Custody