Digital Forensics

Graded Unit: Group Activity

Lecturers: David Nicol/Mark Gillan

The Digital Forensics Process

The digital forensics investigatory process is made up of three main stages:

- Incident response
- Managing digital evidence
- Preparing forensic documentation

Group Activity

- Complete the activity in Groups of 2/3
- Discuss the actions you think should happen at each stage in the Digital Forensics Process.

An Incident has occurred: Incident Response

- Marcus Gillane is an IT technician who works from home for Finnart Street Insurance Services.
- After five years, Marcus Gillane has decided to leave the company because of being successful in gaining a promoted post within a rival Insurance company in Paisley.
- The IT Team noticed during the month before he was due to leave the company, he had downloaded several sensitive files. It has been highlighted that Marcus Gillane has been accessing areas of the company network and files, he would not normally have access privileges for these areas.
- Over the past week the accounts department have recorded that many clients have opted to move to another insurer.
- Some IT equipment has been reported missing by the IT department on Thursday morning. This includes an HP Laptop. From the building access report, it shows that Marcus Gillane was in the building on Wednesday Evening to pick up some personal belongings.

Incident Response

- As lead Investigator, what do you think should be the first actions be in this case?

Incident Response

- As lead digital investigator, how do you prepare for (and also prepare the forensics team for this case?

Incident Response

- Are there any laws which might be relevant/have to be considered at this stage?

Home office of Marcus Gillane

Home office of Marcus Gillane

- What Digital Evidence can be viewed here at the scene?

Home office of Marcus Gillane

- Any other evidence in view (not necessarily digital) which could also be relevant?

Managing digital evidence

- Now that we have access to Marcus Gillane’s Home Office, what preliminary actions should be taken at this stage?

Managing digital evidence

- How do we process the evidence we can view at the scene?

Managing digital evidence

- Is there any other potential evidence which might be relevant (including additional evidence that might not be at this scene)?

Managing digital evidence

- Before analysing evidence – what type of processes should we take?

Managing digital evidence

- During analysing data/evidence, what should we record and continue to keep?

Managing digital evidence

Recording dates and times from digital files and any other electronic evidence can be good for establishing a what during a digital forensics case?

Preparing forensic documentation

In preparing documentation, discuss aspects you think are important for creating a Final Digital Forensics Report (relating to content and presentation).

Digital Forensics Process

To undertake research/further study for the graded unit exam. You should undertake your own research on the three main processes listed below – and add to your study notes.

- Incident response
- Managing digital evidence
- Preparing forensic documentation

Also complete the class exercise provided for Digital Forensics. Make sure work is saved to your Graded Unit OneDrive Folder.