**J0HL34 Digital Forensics**

Learning Outcome One

*Describe incident response procedures:*

* *Secured crime scenes*
* *Sources of digital evidence*
* *Secure recording of actions*
* *Different secure methods*
* *Continuity of evidence (chain of custody)*
* *Relevant legislation*

Due to the continuing Covid19 pandemic we are unable to physically access the crime scene at Glasgow Clyde College this phase. However, here is a picture of the scene, which will allow ourselves to complete the SQA requirements for learning outcome one:



|  |
| --- |
| *Secured crime scenes*  Describe the detailed steps you would have taken if you had to secure the crime scene yourself.  First, I would take preliminary photos to document the undisturbed scene.  Then I would establish and tape of a perimeter that is large enough to cover the relevant area (in this case the desk). I would then secure the room so that no one can enter or exit without authorisation, this is to minimize the risk of evidence tampering. |
| *Sources of digital evidence*  Describe how you would methodically search the crime scene and then record all your inventory and evidence.  I would divide the table into a grid, then using grid reference points I would document all the relevant the items, categorising them into either evidence or inventory. As I am categorising, I would take contemporaneous notes on my findings. As I am documenting evidence I will take photographic and written notes and secure the evidence to be transported back to the lab. |
| *Secure recording of actions*  Describe how you would record your actions with contemporaneous notes.  I would take contemporaneous notes using a Dictaphone. I would start by stating time, date, location and then proceed with a monologue describing in detail in real time what I am documenting along with ID codes. |
| *Different secure methods*  Describe how you would secure digital evidence with for example a faraday bag.  For electronic and storage items (disks etc) where data loss is a risk, I would use a faraday bag and ensure that when handled gloves and a static wrist band are worn. |
| *Continuity of evidence (chain of custody)*  Describe your bagging and tagging process, then in a table record each item with a unique id that relates to the case.    For all the evidence collected I would use labels identifying what it is, an ID number and position it was found. I would also ensure that it was time marked and signed by whoever was gathering the information. When physically handling evidence, I would ensure that gloves are worn and in the case of electronic and storage devices a static wrist band as well.   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | ITEM | ID | Description | Position | Time and Date | Signature | | PC | ID\_01 | Black desktop computer. Make Lenovo Think Centre | A1, top left of desk | 10.06am 9/2/20 | RL | | Handwritten note 1 | ID\_02 | Yellow note attached to computer monitor with the message “Buy something to wipe hard drive.” | A1, on top of PC | 10.07am 9/2/20 | RL | | USB Stick 1 | ID\_03 | Black and purple thumb drive | A2, on top of PC | 10.08am 9/2/20 | RL | | USB Stick 2 | ID\_04 | Black thumb drive | A2, on top of PC | 10.12am 9/2/20 | RL | | Handwritten note 2 | ID\_05 | Yellow page, possible Password? | A2, on top of spiralbound notebook | 10.15am 9/2/20 | RL | | Spiralbound Notebook | ID\_06 | Notebook, may have evidence. | A2, on top of PC | 10.17am  9/2/20 | RL | | Handwritten note 3 | ID\_07 | Yellow page, cannot make out message but may be relevant | A2, at side of PC | 10.19am 9/2/20 | RL | | wikiHow printout 1 | ID\_08 | Document guide can’t make out writing. How to fake an image? | A2, under PC | 10.21am  9/2/20 | RL | | Handwritten note 4 | ID\_09 | White page, note including delete browser history | A2, on PC | 10.23am 9/2/20 | RL | | Hard Drive | ID\_10 | WD hard drive | B1, on shelf behind desk | 10.25am 9/2/20 | RL | | CD 1 | ID\_10 | CD/DVD, not in case | B1, beside PC | 10.27am 9/2/20 | RL | | CD 2 | ID\_11 | CD/DVD, in blue case | B1, beside PC under CD 1 | 10.30am 9/2/20 | RL | | Digital Camera | ID\_12 | Red digital camera with 7 written on it in sharpie | B2, beside CD 1 | 10.32am 9/2/20 | RL | | Tablet | ID\_13 | Black Tablet device in case | B2 beside Digital Camera | 10.35am 9/2/20 | RL | | Mp3 player | ID\_14 | Pink MP3 player may contain audio evidence. E.g., hacking audiobook, conversation recording etc | B2, beside Tablet | 10.38am 9/2/20 | RL | | Black notebook | ID\_15 | Black notebook, containing reference to money | B3, beside MP3 player | 10.40am 9/2/20 | RL | | Laptop | ID\_16 | Silver Dell laptop | C2, to the right of tablet | 10.44am 9/2/20 | RL | | wikiHow printout 2 | ID\_17 | Printed document detailing how to hack a computer | C3, next to laptop | 10.48am 9/2/20 | RL | | Cd 3 | ID\_18 | CD in yellow case half inserted into portable disk drive (which is connected to laptop) | D2, to the right of laptop | 10.52am 9/2/20 | RL |   Inventory items found on desk are monitor A1 unidentified blue square object in A2, keyboard A4 and mouse B4, sticks of RAM at B2 and C3, a set of keys at B2, headphones at C2 (on top of laptop screen) and an orange pen C4. All these items are deemed to be unrelated to the case. |
| *Relevant legislation*  Describe what legislation is relevant and must be followed by yourself at this initial investigation stage.  The Police and Criminal Evidence Act 1984 and Criminal Procedure and Investigations Act must be adhered to. That includes following processes such as chain of custody. |