**J0HL34 Digital Forensics**

Learning Outcome Two & Three

*Scenario*

Gertrude Gray works for White & McKay; this is an online business that over the last few weeks have been struggling to keep their website online.

They suspect it is being flooded with traffic from an internal source, their reasoning for this is that when they disconnect their business from the internet, they still are struggling to keep the server alive! They have done a sweep of their office and internal systems and have found a suspicious USB plugged into Gertrude’s PC.

In addition, Gertrude has found a system service running in the background on her machine and has found this suspicious. This is concerning as her PC contains confidential customer information.

These factors have led to yourself being hired to perform a forensic investigation on the above USB.

*Manage digital evidence.:*

* *Forensically safe working environments*
* *Forensic acquisition*
* *Tools and techniques to obtain digital evidence*
* *System, volatile and non-volatile information*
* *Forensic data analysis from different sources*

*Prepare forensic documentation.:*

* *Justification for forensic investigation*
* *Steps taken throughout an investigation*
* *Evaluation of forensic findings*
* *Recommendations based on findings*

Due to the continuing Covid19 pandemic we are unable to physically access the crime scene for Learning Outcome One this phase. This assessment is a continuation from the scenario detailed for that learning outcome.

For Learning Outcome Two & Three you will need the usb.iso file, as again due to the Covid19 pandemic we are unable to physically provide you with devices to physical acquire data from.

|  |
| --- |
| *Forensic acquisition & Tools and techniques to obtain digital evidence*  *How would the usb.iso file have been obtained from the USB device? What device would have been used to ensure that it could not be tampered with during this process?*  I would take the USB drive and keep that as a master copy, I would then duplicate it to produce a working copy using software for example Passmark’s ImageUSB. Whilst doing the duplication I would use a write blocker (in this case a software write blocker) to ensure that none of the digital evidence is not tampered with. |
| *Forensically safe working environments*  How would you ensure that this orginal usb.iso file is unlikely to be corrupted during your investigation? What cryptographic technique would you use to prove no alteration has occuered from this original?  By creating a back up of the master copy, known as the working copy. This ensures that the original evidence will always remain intact. Through verifying the file integrity via cross referencing the hash file we can ensure that no alteration has occurred from master copy to working copy. |
| *System, volatile and non-volatile information & Forensic data analysis from different sources*  What is the difference between volatile and non-volatile information? What type of information is the usb.iso from?  Volatile information is lost when a computer or device powers down (it’s most likely stored in VRAM) whereas non-volatile information will remain regardless of shutdowns or restarts. The information stored on usb.iso is non-volatile. |
| *Justification for forensic investigation*  What is the background to the forensic investigation? What piece/s of legislation would need to be followed to begin this process?  The main background to the investigation is potential data theft using a computer, leading to a loss of client’s personal information and the interruption of service to White and McKay’s website. This would mean that the Computer Misuse Act 1990 and the Data Protection Act 2018 would need to be followed. |
| *Steps taken throughout an investigation*  Detail what steps you took from the acquisition of usb.iso through to your evaluation of your findings. Detail any forensic analysis performed and tools used  Step one: Opened the iso to find a zip file named files (which is password protected) and a PNG file called password    Step two: The PNG file has image of stenography website.    Step 3: Decoded the PNG file on the website to get the password for the zip folder    Step 4: I unzipped the files to find an excel file and a python file    Step 4: The excel file contains customer’s personal information. It also has for every entry a note that says “needs to be encrypted” which suggests the company of White and McKay are liable for not protecting their customers information securely (therefore breaching the Data Protection Act).  Part of customers stolen data    Step 6: I opened the Python file with IDLE 3.9. The file contains code to execute a Denial-of-Service attack, it also contains the authors pseudonym “Hatty Black”, a reference to being a Black Hat Hacker. |
| *Evaluation of forensic findings*  What did you find during your investigation? Evaluate these findings and include screenshots.  The files contained on this usb show that there has been a malicious attack on the company’s website and a collection of their client’s personal data. Not only this but the company itself may be guilty of not properly encrypting its client’s data in order to protect it. The fact that there is a note saying that this needs to be done shows culpability as the company cannot claim negligence as the need for encryption is clearly stated on each person’s information. In order to ensure the company is liable, we would need a copy of the customer list provided by White and McKay. We could then check the checksum of both files by the hash code and see if there has been any tampering of the file by the hacker. |
| *Recommendations based on findings*  What are your recommendations based on your above findings i.e. which pieces of legislation have been broken?  I find that the hacker known as “Hatty Black” is responsible for breaking the Computer Misuse Act 1990 for the DOS attack and the Data Protection Act 2018 for the theft of personal data. Pending on the result of the checksum test I would find that White and McKay are potentially responsible for not securing their customers data and have therefore broken the Data Protection Act 2018 themselves. |