Module: 216SE - Intermediate Digital Forensics

Coursework

Student ID: 9195071

Contents

Intro

An employee of Coventry University Daelan Dax Deadham is suspected of selling assignments and dissertation writing on the Internet, targeted at Coventry University under and postgraduates. This report will outline the steps that need to be taken in the seizure and storage of digital evidence to ensure its integrity when relied on in legal proceedings.

Plan

Entry

To gain access to the EC3-39 room in the Engineering and Computing building under section 8.1 of the code of practice of the power of entry, reasonable notice should be given to the owner of the building (Coventry University) before exercising the entry power (gov.uk, 2014). If there has been a warrant issued for the search of these premises the search must be carried out within 3 months of the issue according to PACE code B section 6.1 (gov.uk, 1984). The search should also be carried out at a reasonable hour according to section 6.2 of PACE (gov.uk, 1984).

If the subject of the warrant is present when the officers arrive copies of the warrant and notice should be provided to them according to section 6.8 of PACE (gov.uk, 1984). All ACPO principles should be followed during this time to preserve the integrity of any evidence found.

Sources of Evidence

According to the brief provided, Daelan Dax Deadham has been provided with a company-issued HP desktop computer and a company-issued HP Zbook15 laptop. While it is very likely both of these are open systems care should still be taken in preserving their state in case they are closed systems. As the office is a shared space there will be other devices present that do not fall under the scope of the search. If there are devices powered on in the room with information displayed pictures of the screens while applying ACPO principle 1: 'No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court' (ACPO, 2012).

Care should be taken when looking for additional sources of evidence. According to the pictures provided in the brief, the office is in an untidy state and has many boxes in which devices could be hidden. The additional sources of evidence to look for include but are not limited to Mobile phones, CDs, DVDs, USB drives, SD cards, RFID Tags or GPS systems such as a smartwatch.

Evidence Acquisition and Preservation

Not every digital device in EC3-39 will be part of the investigation so care must be taken to make sure that any seizure is 'justified, appropriate and proportionate' (Marshall, 2009). Any device that is deemed to contain evidence should be cordoned off to minimise the risk of it being tampered with. This will also remove the potential for accusations of planting evidence to arise during the investigation (Marshall, 2009).

All systems found should now be checked for signs of being a 'live' system. If the system has software running or has visible signs of power running to the device, pictures should be taken and no effort to change the running of the system such as getting rid of a screensaver should be made. A cable trace should be done on the system in question to find obvious signs of it being connected to a network, general advice at this stage is to remove the system from the network by unplugging the cable (Marshall, 2009). This is left to the lead investigator on-site following ACPO principle 4: 'The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to' (ACPO, 2012) as there is also a risk a loss of network connectivity could trigger a massive irretrievable data loss. If any action should be taken on the live device, all actions should be logged in the audit trail to allow examiners to account for anomalies in the data. All cables that lead to the device should be labelled accurately too.

On these live systems, RAM data should be a top priority to be captured and stored as it is the most likely to be lost in the case of a power outage or system shutdown. Ram analysis is important in this case as it may contain:

- browsing history
- encryption keys
- chat messages
- clipboard contents
- run-time system activity
- open network connections (often these artefacts are only found in RAM)
- recently executed commands and processes
- injected code fragments
- memory stored before shut down or crash

(ADF Solutions, 2018)

All of which could harbour evidence of selling of essay writing on chat rooms or messaging services.

If powered off investigators can perform static analysis on the devices. When taking a copy of the storage device a write-blocker should be used and connected to the imaging workstation to prevent alteration of the data. A control master sample and should be made with the write blocker and then from this a copy is generated to work on. All images should be verified with a HASH, most of the time MD5. In accordance with ACPO principle 2: 'In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions' (ACPO, 2012).

Equipment for evidence acquisition

Many tools need to be used to preserve the evidence gathered in this investigation. Multiple redundancy copies of these tools should be carried as well to make sure the investigation goes without interruption or complication.

- A write-blocker (physical) to aid in the collection of data while preventing the alteration of data.
- Gloves to preserve the crime scene as the room ED3-39 should be treated as such.

- Forensically sound bootable CD's and DVD's.
- Forensically sound (Ideally in shrink wrap) flash drives.
- A hub or switch with networking cables to set up a makeshift network in the crime scene if necessary.
- A Field logbook with pens.
- More assorted cables for video/sound/power/mobile connectivity.
- A Digital camera to capture live data on screens.

Summary

In summary, the investigators on this case should try their best to adhere to ACPO principles at all times. All authority should be signed and ready to produce for any purpose. The desk belonging to Daelan Dax Deadham should be identified before any other action is taken. All identified systems should be cordoned off to prevent tampering with evidence. If any of these systems are deemed as live, pictures of the state of the system should be taken along with whatever they may be displaying on any screen. Each system should be identified correctly with the case handler signing off each system.

When devices are seized to collect evidence the seizure should be justified and appropriate with the subject of the investigation being informed and handed a copy of the notice and warrant. All evidence should be verified with hashes to ensure their integrity further on in the investigation. All physical devices seized from the scene should be placed in evidence bags and correctly labelled.

All investigators should keep their own copy of contemporaneous notes that should be compared and documented to avoid the possibility of evidence tampering. This is in accordance with ACPO principle 3: 'An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result' (ACPO, 2012).

References

ACPO Good Practice Guide for Digital Evidence. (2012). https://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf.

ADF Solutions. (2018). Don't Forget RAM Capture: A Key to Digital Forensics. https://www.adfsolutions.com/news/ram-capture.

gov.uk. (1984). POLICE AND CRIMINAL EVIDENCE ACT 1984 (PACE) CODE B. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/903811/pace-code-b-2013.pdf.

gov.uk. (2014). Power of Entry. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/383079/Code_of_Practice_-*Powers_of_Entry__web*.pdf.

Marshall, A. (2009). Digital Forensics. John Wiley & Sons.