Forensic Science Regulator
Overseeing Quality

Lessons Learnt

Issue 1/ 2019

Evidence handling error

Key Words: Digital, Fishbone or Ishikawa diagram, Hard disk, Wiped.

A digital forensic company, tasked by the defence, sent a hard disk to the forensic unit tasked by the prosecution to copy the image files of an exhibit. Upon receipt, the prosecution's forensic unit attached the drive to a forensic workstation. They noticed that the hard disk contained an operating system on a partition that took up approximately 100GB of the 250GB hard disk's capacity.

On an initial review of the copied images the disk contained a full operating system. The forensic unit believed that this operating system was restored on to this disk from a possible indecent images investigation. Any person who plugged this hard disk into their computer would be able to see these pictures. They deemed that the hard disk was not suitable to copy the exhibit on to, as it had not been forensically wiped.

The forensic unit contacted the party that had instructed the sender of the disk.

Investigation

When the drive was returned to the defence's forensic unit, they identified the case that the data came from. Three analysts worked on the original case and the case notes included details of cloning of drives contained in the exhibit during September 2016. In the case file there was a mention of failed clones; however, there was no record of this particular drive being cloned.

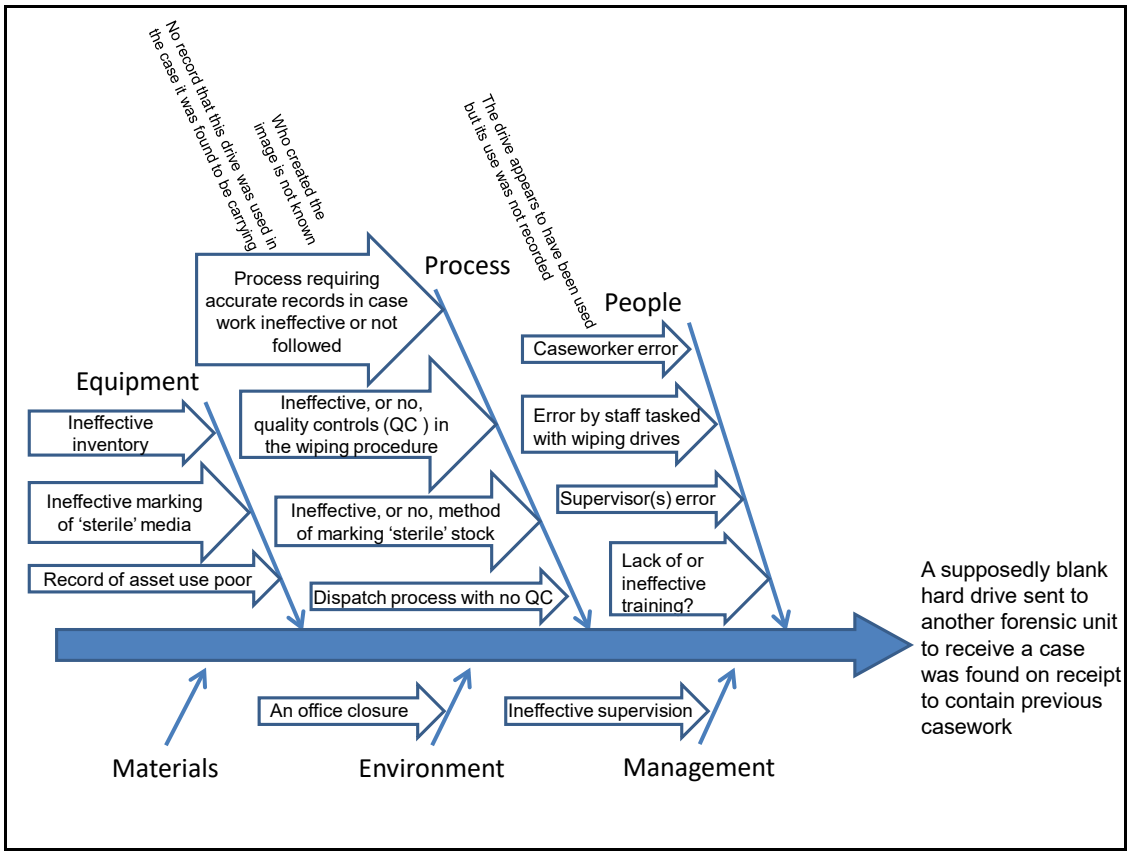
The process should be that when data are no longer required the used drives should be placed in the area/folder marked 'To Be Wiped'. Once wiped they should be

placed in a new evidence bag and sealed with a label. This does not appear to have happened. The initial finding of the root cause was 'user error'.

Root cause

There were multiple errors in this case, but the root cause was not simply human error. The initial caseworker(s) did not record that the drive in question was used. Also, it was not clear in the records as to which of the individuals listed actually attempted to create a cloned image. 'Someone' was tasked to wipe drives in advance of an office move; this did not happen and the process was not overseen or supervised. The processes in place in the casework, inventory management and dispatching drives to third parties were either ineffective or not followed. A verdict of 'user error' is not a finding that is accepted by the Forensic Science Regulator. However, the investigation did identify process changes, which appeared to be an acceptance that this was a more systemic issue.

There are many methods for assisting in the investigation of the root cause of incidents, including the 'five whys' and more visual ones such as the Fishbone diagram or Ishikawa diagram below.



Things to consider

1) Every copy of casework must be accounted for.
2) Caseworkers need to make accurate records of any exhibits handled and copies made.
3) If new media cannot be used, drives need to be wiped and clearly marked as such.
4) The level of seriousness of a non- sterile drive leaving the premises means a quality assurance step
5) Must be included if new media are not used.
6) Forensic units receiving blank drives to copy cases on to need to have a procedure to follow should they receive a 'non-sterile' drive. This will normally be contacting the sender directly and immediately.
7) Casework must only be transferred between forensic units in a secure manner.

Relevant documents

Codes of Practice and Conduct:

www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct#codes-of-conduct-and-practice

Digital Forensic Services: Codes of Practice for forensic science providers

www.gov.uk/government/publications/digital-forensic-services-codes-of-practice-for-forensic-service-providers

Guidance on legal obligations

www.gov.uk/government/collections/fsr-legal-guidance

FSR Newsletter (Issue 30)

www.gov.uk/government/publications/forensic-science-regulator-newsletter-number-30

ISO 17025

www.iso.org/home/standards/popular-standards/isoiec-17025-testing-and-calibra.html

You may also wish to visit The Chartered Society of Forensic Sciences website: www.csofs.org/