|  |  |
| --- | --- |
| Lesson: 6 – Collection of electronic evidence | **Duration: 150 Minutes** |
| **Resources required for an off-line delivery:**   * Laptop or PC running an operating system with an office suite (capable of showing pptx) * Projector and display screen * Internet access (if available) * Whiteboard * Whiteboard pens (at least 2 each of blue, black, red and green) * 2 Flipcharts with adequate paper * Student notepaper and pens * Blu tack or a similar product to allow for paper to be affixed to the walls temporarily * Files: Session 6 Collection of Electronic Evidence.pptx   **Resources required for an on-line delivery:**   * Laptop or PC for each trainee (if attending from home) or for a groups of trainees, depending on availability * A strong internet connection * An online tool should be provided that allows video conferencing and is specifically aimed at providing training. Due to the fact that the trainers have to stay in visual contact with the trainees, it is important that when the slides are shown, the trainers still see the trainees (in some online video conferencing tools only the slide can be seen). It is in any case also a plus to be able to provide online break-out rooms. * Files: Session 6 Collection of EE.pptx | |
| **Aim:** This session will cover the technical principles of the collection of electronic evidence. Although these principles remain largely similar across jurisdictions, this course has been developed with the aim of standardising our approach and is based on internationally recognised international standards such as ISO/IEC 27037 and the NIST Guide to Integrating Forensic Techniques into Incident Response. | |
| **Objectives:**  At the end of this session, delegates will be able to:   * Explain which measures need to taken in order to preserve evidence and prepare for its collection * Identify sources of electronic evidence * Discuss options for recovery data from physical storage media as well as cloud storage * Be aware of the challenges posed by encryption * Describe the processes of seizing, imaging and hashing data * Distinguish between Live data forensics and post mortem forensics * Illustrate the importance of the chain of custody * Discuss data retention policies | |
| **Introduction**  In other CoE courses the focus of the hardware related sessions is on the identification of devices, the technical description of services on the Internet and the potential evidence which may be found on the different devices as well as the practical usage of services and technologies. This session focusses on how to prepare for the capture and how to collect that evidence from different devices and world wide web services.  This session covers the following topics:   * Preservation of evidence * Preparation for collection * Identification of evidence * Recovery from physical storage devices * Recovery forensics from the cloud * System administators * Encryption and decryption * Seizure of systems and devices * Imaging * Hashing * Live forensics vs dead (post-mortem) forensics * Chain of custody of electronic evidence * Data retention   All information about this session is included in the PowerPoint presentation entitled “Session 6: Collection of electronic evidence.pptx” in the resource pack. The trainer is responsible for ensuring that the materials are up to date. Changes may be made, however the objectives should be achieved. | |
| **Practical Exercises**  There is only one small practical exercise foreseen in this session. Since this is very short and straightforward exercises, the instructions for them included on slide 6 and in the comment section of slide 7. | |