|  |  |
| --- | --- |
| Lesson: 10 – Collection of electronic evidence | **Duration: 120 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 10 - Examination and Analysis of Electronic Evidence.pptx   forensic\_analysis\_examination\_1\_voice\_over.mp4  forensic\_analysis\_examination\_2\_voice\_over.mp4  forensic\_analysis\_ram\_sneakpeak\_voice\_over.mp4  forensic\_analysis\_registry\_voice\_over.mp4  **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 10 - Examination and Analysis of Electronic Evidence.pptx | |
| **Aim:** This session will showcase examples of techniques that can be used to examine analyse computer and mobile systems. The participants should get a better overview of what is possible in digital forensics and which evidential data can be extracted from computer and mobile systems. | |
| **Objectives:**  At the end of this session, delegates will be able to:   * Distinguish between traditional computer forensics and mobile forensics * Discuss options for the storage of digital evidence * Describe considerations for determinining the volatility * Outline procedures to collect log files * Summarise the evidential items which can be found digital devices * Summarise options for decrypting data * Discuss different documentation techniques * Identify methods for physical and logical extractions * Distinguish between different levels of examinations and analysis techniques * Describe techniques to analyse hidden data, application data and files * Identify methods to analyse e-mail evidence and network traces * Summarise the elements of a forensic report | |
| **Introduction**  This session is split in three parts. The first short introductory part shows the different areas in the field of digital forensics and outlines some of the differences between computer forensics and mobile forensics. The second part will give examples of challenges, analysis techniques and evidential items that can be found when analysing a computer system. The third part has a similar focus as the second part, but it concentrates on mobile devices.  This session covers the following topics:   * Storage of evidence * Determination of volatility * Collection logs * Decryption * Documentation * Physical & logical extraction * Temporal analysis * Relational analysis * Functional analysis * Timeframe analysis * Data hiding analysis * Application and file analysis * Log Files analysis * Email analysis * Network analysis * Preparation of report (scope, contents, organisation)   All information about this session is included in the PowerPoint presentation entitled “Session 10 - Examination and Analysis of Electronic Evidence.pptx” in the resource pack. There are also pre-recorded videos available for this session:  forensic\_analysis\_examination\_1\_voice\_over.mp4  forensic\_analysis\_examination\_2\_voice\_over.mp4  forensic\_analysis\_ram\_sneakpeak\_voice\_over.mp4  forensic\_analysis\_registry\_voice\_over.mp4  The trainer can use them throughout part 2. There are notes in some slides indicating a potential use of a video.  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 no practical exercise in this session. However, an experienced trainer can decide to deliver the whole session via live demo showcasing the analysis of a case in a forensic software. | |