EC-Council

Report generated on : 18 Dec 2023 01:51 AM

Player Details

User	**James5309**
Lab Id	7120867225239425284
Lab name	DFEv1 Module 05 Defeating Anti-forensics Techniques
Score	**40**
Possible score	40
Date played	19 Oct 2023 20:24 PM

Flag Details

Name	Course	Task	Status	Hints used	Score
Use EaseUS Data Recovery Wizard tool available at Z:\DFE Module 02 Computer Forensics Investigation Process\Data Recovery Tools\EaseUS Data Recovery Wizard to recover data from lost/deleted partitions in the Windows 10 machine. Enter the total number of .mp3 files available at Lost Files -> Lost Partition -> Audio Files location.	Digital Forensics Essentials v1	Understand Anti-forensics and its Techniques	Completed	0	**10/10**
Install Passware Kit Forensic tool in Windows 10 machine to crack the passwords of password-protected files and applications. Crack the password of file Sample_1.docx available at Z:\Evidence Files.	Digital Forensics Essentials v1	Understand Anti-forensics and its Techniques	Completed	0	**10/10**
Use the Autopsy tool on the Windows Server 2019 machine to perform SSD file carving on a Linux file system. Retrieve carved files from the evidence file Linux_Evidence_SSD.dd available at C:\DFE-Tools\Evidence Files\Forensic Images. Enter the last four digits of the MD2 hash value of the f0203080.jpg image (8fe73068c8b7ae80232d4c548b9dXXXX).	Digital Forensics Essentials v1	Understand Anti-forensics and its Techniques	Completed	0	**10/10**
In Windows Server 2019 machine, use StegSpy tool available at C:\DFE-Tools\DFE Module 05 Defeating Anti-forensics Techniques\Steganography Detection Tools\StegSpy to detect steganography. Analyze Model.png suspicious file available at C:\DFE-Tools\Evidence Files\Image Files and enter the marker position where steganography is found.	Digital Forensics Essentials v1	Understand Anti-forensics and its Techniques	Completed	0	**10/10**

Target Details

Name	Operating System
DFEv1 Ubuntu Suspect	Linux
DFEv1 Ubuntu Forensics	Linux
DFEv1 Windows 10	Windows