# EC-Council

Report generated on : 18 Dec 2023 01:50 AM

## Player Details

| | |
|---|---|
| User | **James5309** |
| Lab Id | 7140561138880708868 |
| Lab name | DFEv1 Module 04 Data Acquisition and Duplication |
| Score | **40** |
| Possible score | 40 |
| Date played | 13 Dec 2023 04:40 AM |

## Flag Details

| Name | Course | Task | Status | Hints used | Score |
|---|---|---|---|---|---|
| Create a dd image of the primary disk/internal disk (PHYSICALDRIVE0) of the Windows 10 virtual machine using the dd command. Use a secondary physical disk (PHYSICALDRIVE1) as an external storage device to store the image. (No answer is required. Write skip as an answer to skip this flag) | Digital Forensics Essentials v1 | Discuss Different Types of Data Acquisition | Completed | 0 | **10/10** |
| Install qemu-utils tool on the Ubuntu Forensics machine. Convert an acquired image file (Windows_Evidence_002.dd) available at DFE-Tools\Evidence Files\Forensic Images to a bootable virtual machine. (No answer is required. Write skip as an answer to skip this flag) | Digital Forensics Essentials v1 | Understand Data Acquisition Methodology | Completed | 0 | **10/10** |
| Use Belkasoft RAM Capturer tool available at Z:\DFE Module 04 Data Acquisition and Duplication\Data Acquisition Tools\Belkasoft RAM Capturer for RAM acquisition on the Windows 10 machine. Enter the size of the physical memory page. | Digital Forensics Essentials v1 | Understand Data Acquisition Methodology | Completed | 0 | **10/10** |
| Use the AccessData FTK Imager tool available at C:\DFE-Tools\DFE Module 04 Data Acquisition and Duplication\Data Acquisition Tools\AccessData FTK Imager to view the content of forensic image file. View the content of the forensic image (Windows_Evidence_001.dd) available at C:\DFE-Tools\Evidence Files\Forensic Images. Enter the physical size of the 1200px-Peace_sign.svg.png file. | Digital Forensics Essentials v1 | Understand Data Acquisition Methodology | Completed | 0 | **10/10** |

## Target Details

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