Blue Team Level 1 Certification (Standard)

8 Topics | 1 Quiz
DF4) Windows Investigations
3 Topics | 3 Quizzes
DF5) Linux Investigations
4 Topics | 2 Quizzes
DF6) Volatility
3 Topics | 1 Quiz
DF7) Autopsy
4 Topics | 1 Quiz
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
SI1) Introduction to SIEM
7 Topics | 1 Quiz
SI2) Logging
6 Topics | 2 Quizzes
SI3) Aggregation
2 Topics | 1 Quiz
SI4) Correlation
6 Topics | 1 Quiz
SI5) Using Splunk
5 Topics | 2 Quizzes
INCIDENT RESPONSE DOMAIN
IR1) Introduction to Incident Response
8 Topics | 1 Quiz
IR2) Preparation Phase
10 Topics | 2 Quizzes
IR3) Detection and Analysis Phase
7 Topics | 4 Quizzes
IR4) Containment, Eradication, and Recovery Phase
5 Topics | 1 Quiz
Section Introduction, CER
Incident Containment
Taking Forensics Images
Identifying and Removing Malicious Artifacts
Identifying Root Cause and Recovery
Activity) End of Section Review, CER
IR5) Lessons Learned and Reporting
7 Topics
IR6) MITRE ATT&CK
13 Topics | 2 Quizzes
BTL1 EXAM
Exam Preparation
Using RDP and SSH
How to Start Your Exam

Taking Forensics Images

Blue Team Level 1 Certification (Standard) > IR4) Containment, Eradication, and Recovery Phas... IN PROGRESS

It's important to preserve as much evidence as possible so that defenders can learn from an incident by determining what tactics, techniques, and procedures (TTPs) were used, and collect indicators of compromise which can be shared with other organizations to help them defend themselves from similar attacks. Forensic images should be taken of the hard drives of affected systems, and also memory dumps to capture any artifacts that may be in RAM.

In some cases, the forensic image of the drive may be stored on a USB so that multiple analysts can analyze it, and make it easier to store, as opposed to only having one copy on a forensic laptop or workstation.

FTK IMAGER & KAPE

In the "**Disk Imaging: FTK Imager**" and "**Live Acquisition: KAPE**" lessons within the Digital Forensics domain we covered how to collect memory and take a disk image using these tools. If you want to read an in-depth explanation of evidence collection, we recommend you complete these lessons before this one, as it's the same process for incident response. We'll provide a shorter overview below on how forensic images would be taken.

In a real-world situation, an incident responder with digital forensics skills would gain access to the affected system or systems, and use KAPE to quickly collect evidence from volatile locations such as RAM. Hard drives would then be connected to a hardware write-blocker, which is connected to a forensic laptop or workstation. This allows the forensic analyst to take a bit-by-bit copy of the hard drive without their device altering anything on the suspect drive. Hashes will be compared between the original drive and the disk image to ensure that they are exactly the same. The newly-generated disk image will then be copied, and the original will be placed into secure storage, allowing analysts to investigate a copy of the disk image, preserving both the original evidence and the initial copy. The forensics analysts will then collect evidence as covered in the "**Digital Evidence Collection**" section of the Digital Forensics domain.

VIRTUAL DESKTOPS

If users are not using physical devices, and instead working on virtual desktops, such as Citrix environments, we would take a different approach to gather a disk image for later analysis and evidence collection. In this circumstance, we would take a snapshot of the virtual system, mount this snapshot in another virtual machine designed with forensics in mind, such as Sift, and then take a disk image of the mounted snapshot.

‹ Previous Topic
Mark Complete ✓
Next Topic ›
Back to Lesson