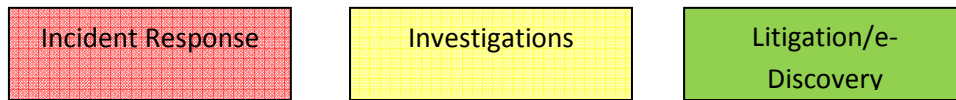
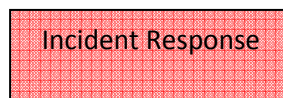


EnCase Enterprise can be used for many different things, but its use can generally be categorized into one of three different categories:



Depending on what type of task you need to perform, each category has different recommended steps. The following steps are just the ***initial recommended actions*** you can take at the offset of your investigation. These steps are not meant to be inclusive of everything you could do in a particular situation, but rather, a starting point and guide to get you started.



An incident response investigation usually involves quickly triaging and examining several different machines for symptoms of a particular incident. For example, it may be to see if any machines in your network have a particular known malicious application running. It could also be to check for a specific registry entry or file that may exist in a specific location that is known to be attributed to malicious behavior.

- Step 1. Execute the "Sweep Enterprise" EnScript located in the EnScript/Enterprise folder
- Step 2. Supply the necessary information and a unique bookmark name to store the collected information. Connect to the appropriate SAFE and use the appropriate ROLE.
- Step 3. Enter the IP addresses, machine names or IP ranges of the machines you want to sweep. You can enter them manually, or click on the Network tree button to see a list of defined IP addresses & ranges.
- Step 4. You can leave the module list empty unless you want to search for a specific registry key (scan registry module)
- Step 5. Choose the sweep options and make sure the "Get Snapshot" option is selected from the "snapshots" tab. Also, define how many connections you will use. The more connections, the faster the sweep.
- Step 6. Click on Finish and watch the status window until it completes. You can review the results by going to the Bookmarks->[bookmark name you provided]->snapshots tab
- Step 7. Using conditions and filters, you can quickly identify specific hosts that match any certain criteria that you may want to define, i.e. a specific running process, open port or user account.

Investigations

An investigation usually involves at least one person and computer. The purpose of an investigation could be to determine misbehavior either at the corporate level or criminal level. This type of action usually involves a more detailed analysis of the computer system and the files and folders contained on all the media related to that person.

Depending on the exact type of investigation, you may want to collect volatile data prior to performing any analysis. This would preserve the state of the machine, the processes running and state of the network. If the nature of investigation involved applications such as internet history, instant messaging clients, email, etc, then it would be a good practice to collect the snapshot data AND an image of memory for preservation.

- Step 1. Collect snapshot data using the exact same procedure that was detailed in the incident response process
- Step 2. Click on “Add Device”, choose the physical memory checkbox and the local drives option. Choose the physical or logical drive and the “RAM object that you want to acquire or analyze and choose next.
- Step 3. Once the objects have been added into EnCase you can decide to acquire them to make a copy (image) or do a live analysis.
- Step 4. This next step ultimately depends on what type of investigation you are performing, but general starting points can be:
 - i. Keyword Search
 - ii. Review Internet History
 - iii. Review Email
 - iv. Review User-created files (docs, multimedia, etc.
 - v. Review LNK files
 - vi. Anti-virus scan

Litigation/e- Discovery

Litigation/e-Discovery usually has the specific purpose to collect and preserve files of certain types and from certain people (custodians). This type of process is very specific and usually does not require any detailed analysis. This process will require connecting to each machine, previewing the attached media, selecting the files based on some previously defined criteria and then creating a logical evidence file that only contains the files/information you need. For example, some typical criteria may be to collect all Microsoft Word Documents, or all PDF files, or all files with a specific keyword inside.

- Step 1. Click on “Add Device”, select the “sessions” checkbox. You can now enter each specific IP address of the machines you need to process or enter and process each one separately. In either case, enter the IP address and then choose NEXT
- Step 2. Chose the logical drives of the media you want to process and click NEXT and FINISH
- Step 3. Once added to EnCase as a preview, you can now use filters, conditions or keyword searches to refine and identify the files that match the criteria that were previously defined.
- Step 4. Keep in mind that if you are using keyword searches to identify specific files that have that text, you may have to use 3rd party utilities to process complex files such as PDF files and email message stores. These files can be searched in EnCase, but there are 3rd party utilities that can search quicker and more accurately than using EnCase.
- Step 5. Once you have selected (blue check) the files that you want to collect, right click in the TREE PANE (upper-left) and choose “Create Logical Evidence File”. Supply the necessary information in the acquisition window and a path for the resulting logical evidence file (LEF). The file will be created with a .L01 extension and can be loaded and read using EnCase.