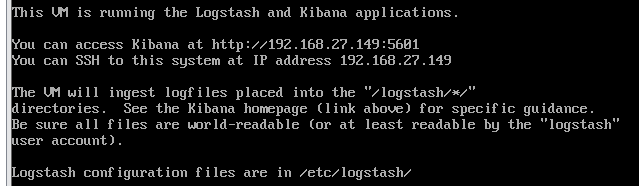
****

The SOF-ELK VM can be downloaded from <https://github.com/philhagen/sof-elk/blob/main/VM_README.md>

Once the VM is downloaded and booted, take note of the GUI IP and the SSH IP. The IPs might fall off the screen during configuration



After booting the VM run the update script to update any configuration files - /usr/local/sbin/sof-elk\_update.sh

In its current state, the VM will only hold 50gb of artifacts. Increase the VM’s disk size to 700gb and then increase the size of the partition that receives the artifacts. This will increase the size of the partition that receives the artifacts to 250gb.   
  
sudo –s (persist sudo mode)

Yum install cloud-utils-growpart (utility we will use to grow the partition).

Growpart /dev/sda 2

Pvresize /dev/sda2

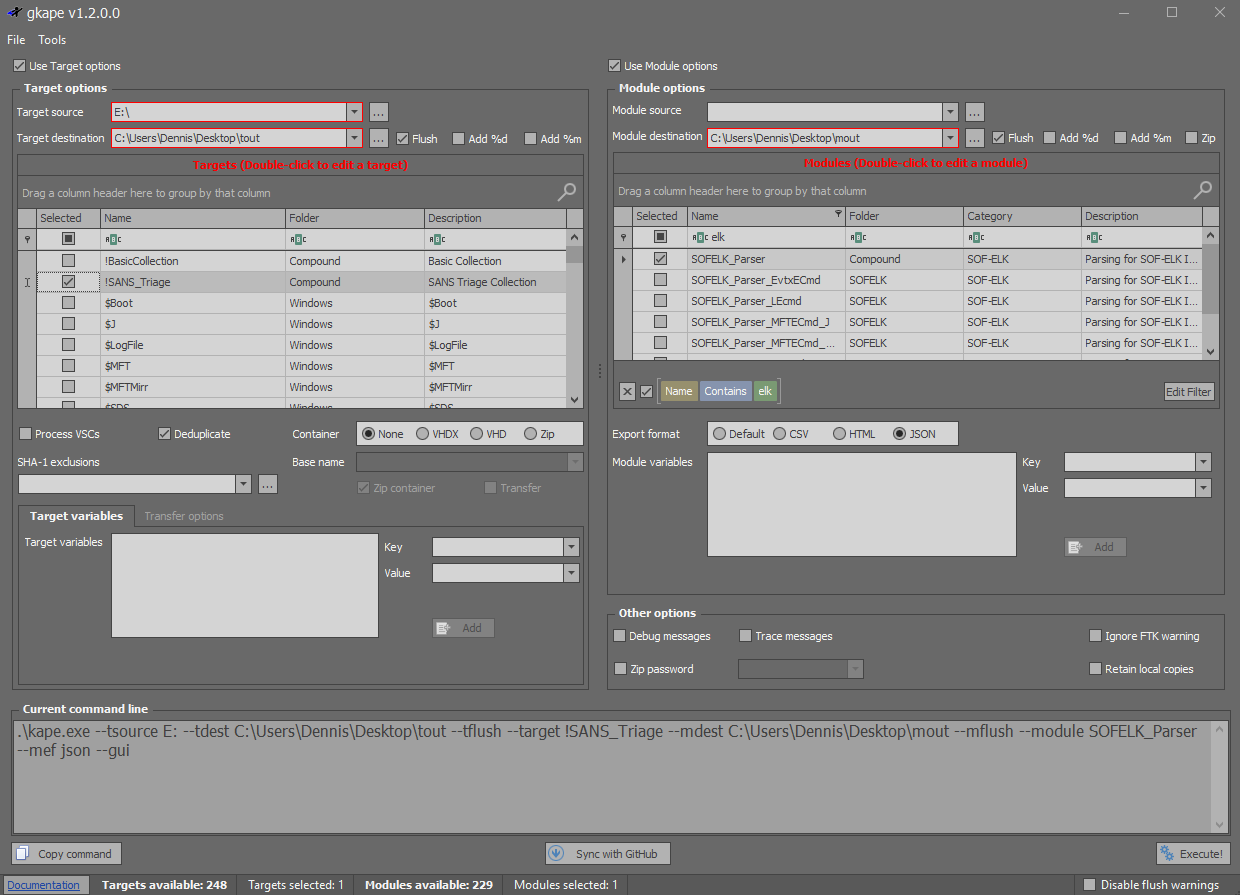
Lextend /dev/mapper/centos\_sof--elk-root -|+100%FREE –r

The easiest way to get your SOF-ELK instance back to a clean state (clear index) is to create a snapshot of the VM at this time.   
  
Before we copy our data over to SOF-ELK, we should stop the logstash service. This prevents logstash (the service indexing the data) from indexing a file that has not finished uploading.

systemctl stop logstash

The logs you are ingesting will determine where you will upload the data. In this example we will use KAPE output.

Point KAPE target source at the image you have collected (and mounted) and run !SANS\_Triage as the target, and the SOFELK\_Parser as the module. Make sure you set the Export Format to JSON.

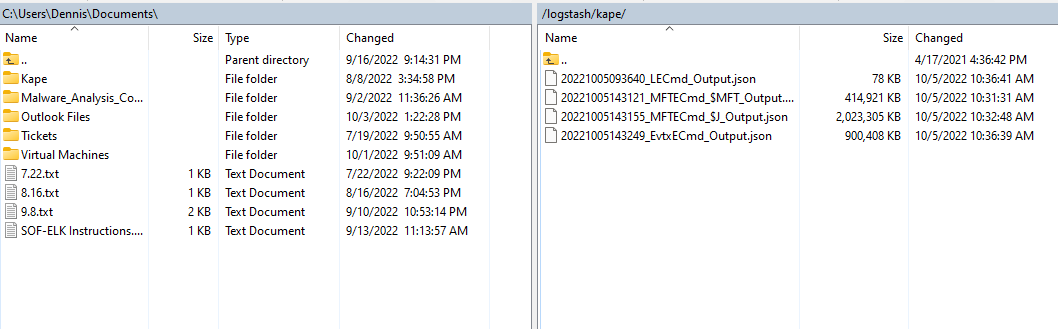


The SOFELK\_Parser module will processes the image Event Logs, .LNK files, $MFT, $UsnJrnl, and Prefetch, and output 4-5 (no prefetch by default on Windows Server) respective JSON files.



.\kape.exe --tsource E: --tdest C:\Users\Dennis\Desktop\tout --tflush --target !SANS\_Triage --mdest C:\Users\Dennis\Desktop\mout --mflush --module SOFELK\_Parser --mef json --gui

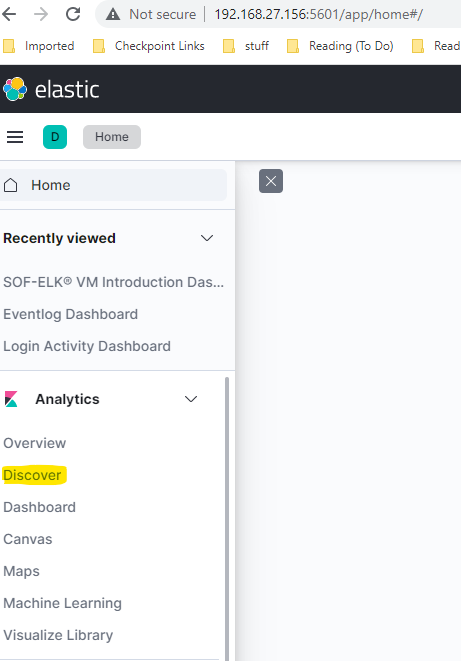
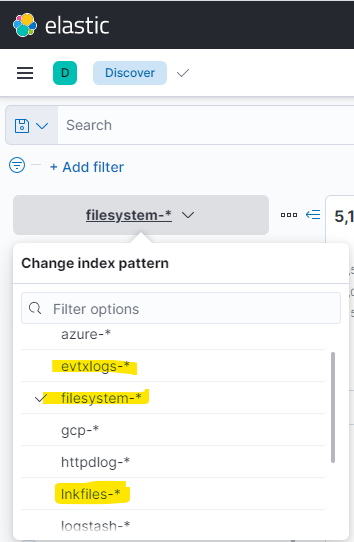
We can now SFTP into the VM and drop the JSON files into the /logstash/kape folder.



In the VM, type systemctl to start logstash. The indexing is impressively fast, usually only taking a couple minuets to index the data.

Once the data has finished indexing (there won’t be any notifications, just give it a few minutes before digging in) use a browser to access the GUI front end with the IP and port that was displayed when the VM booted.

In the “Discover” page is where you will find your data that has been indexed along with the different index patterns that we uploaded

When you are done with your analysis, revert the VM to the post configuration snapshot for a clean index.

Resources:

Kibana Query Language - https://www.elastic.co/guide/en/kibana/master/kuery-query.html

SANS Presentation - https://www.youtube.com/watch?v=Hk6An-LJ4jY