Lab 0: Install SOF-ELK® VM

Objectives

- Install the SOF-ELK® virtual machine (VM) on your Windows workstation
- Configure and start the SOF-ELK® VM
- Load MaxMind's GeoIP database
- ***Update the SOF-ELK VM & Workbook***
- Access Kibana via your host's web browser

Background

Logs can be viewed within each cloud's console. However, most companies prefer the "single pane of glass" approach and combine all logs in a Security Information and Event Management (SIEM) system. For the our class, we chose ELK as our SIEM. We specifically selected the SOF-ELK distribution as it's maintained by SANS instructor Phil Hagen and includes numerous parsers that we need to ingest cloud logs.

Preparation

To prepare:

1. Install VMware Workstation or VMware Player from vmware.com
    - https://www.vmware.com/products/workstation
    - https://www.vmware.com/prodcuts/player
2. ***Be sure to install version 15.x or later. Earlier versions will not work correctly on Windows 10***
3. Make sure you have at least 40GB of available disk space
4. SOF-ELK is based on CentOS:
    - ***Do not change your regional or time settings inside the VM***
      The VM is preconfigured for the UTC time zone which is best practice for forensic investigations.
    - ***Do not update the operating system***
      The labs have been tested based on the exact version of SOF-ELK provided to you. Any changes may alter the results and impact your educational experience.
    - Feel free to give your VM additional CPU and/or RAM
5. SSD storage is highly preferable if available on your laptop.

Install Steps

1. Install 7-Zip on your workstation

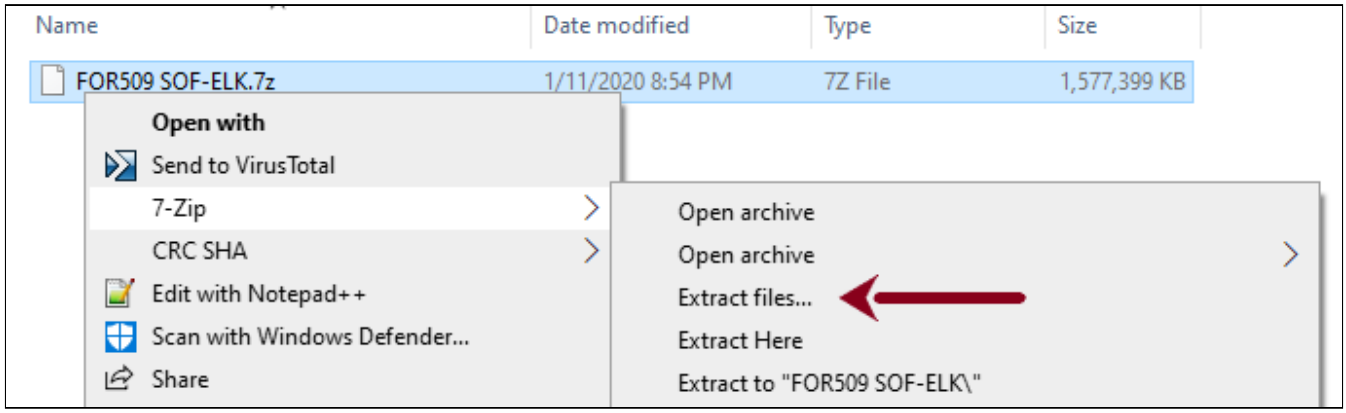
   The SOF-ELK VM will be provided to you in a compressed format and require the 7-Zip utility to decompress.

   - https://www.7-zip.org/

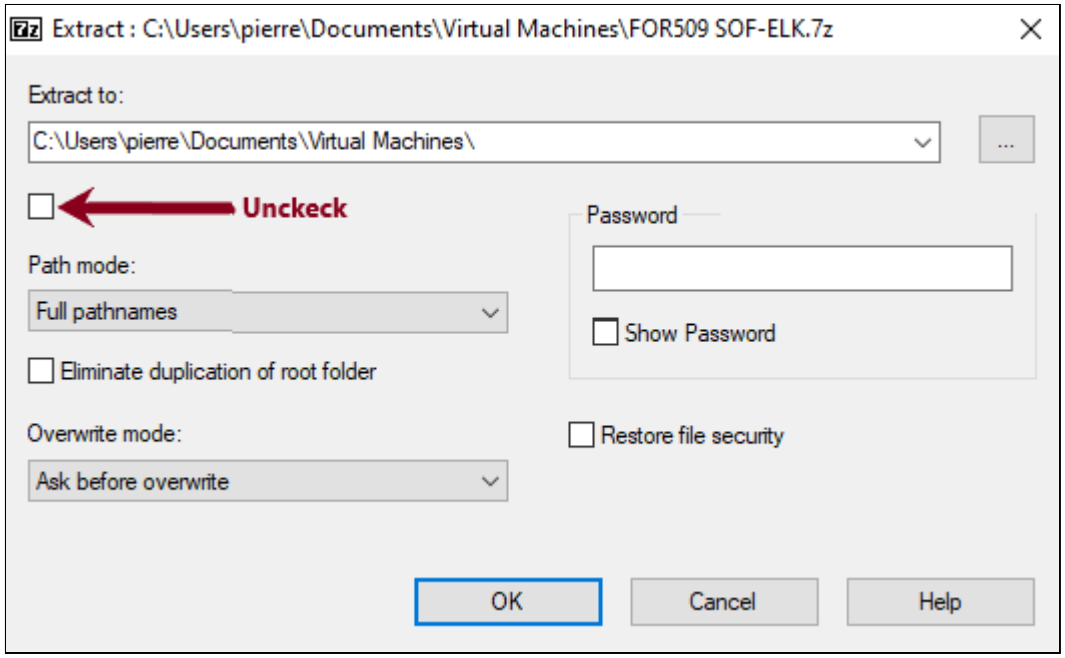
2. Unzip the SOF-ELK VM

   The VM may be provided to you either on a USB drive or as a download link in your SANS portal depending on your class modality. You will need to unzip the `FOR509 SOF-ELK.7z` file to your `Virtual Machines` folder on your host:

   - Right-click the file to get the 7-Zip options and select `Extract Files...`



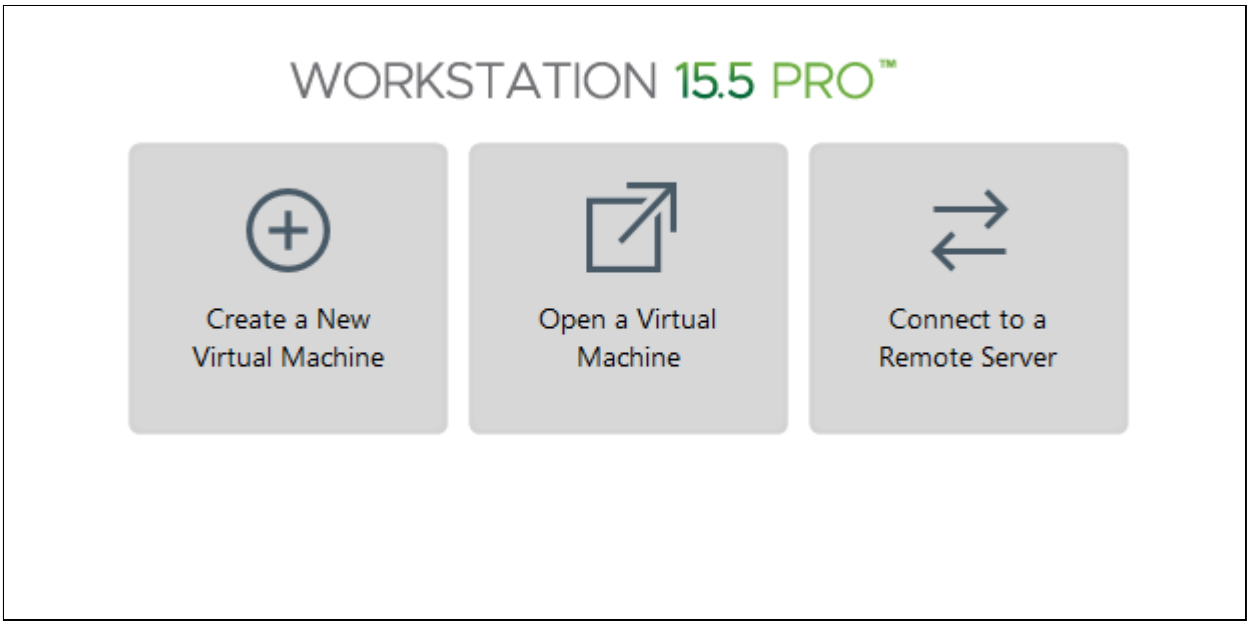
   - Select a folder on your system to extract the files to
     - Recommend `c:\Users\<Username>\Documents\Virtual Machines`
   - Uncheck the checkbox below the `Extract to:` path



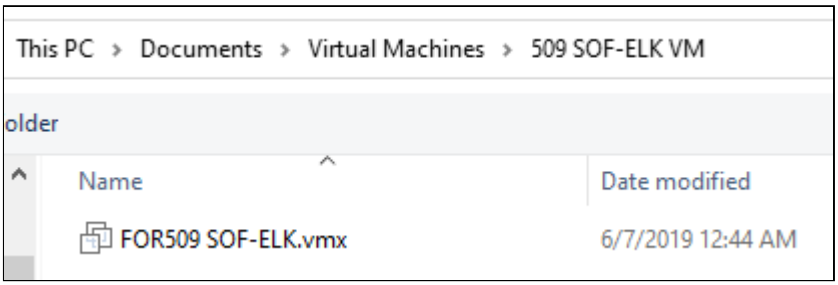
- Depending on whever you have an SSD drive or not, the extraction process can take between 5 and 20 minutes. Once completed, you will have a folder called `c:\Users\<Username>\Documents\Virtual Machines\509 SOF-ELK VM`

3. Configure VM Hardware Settings

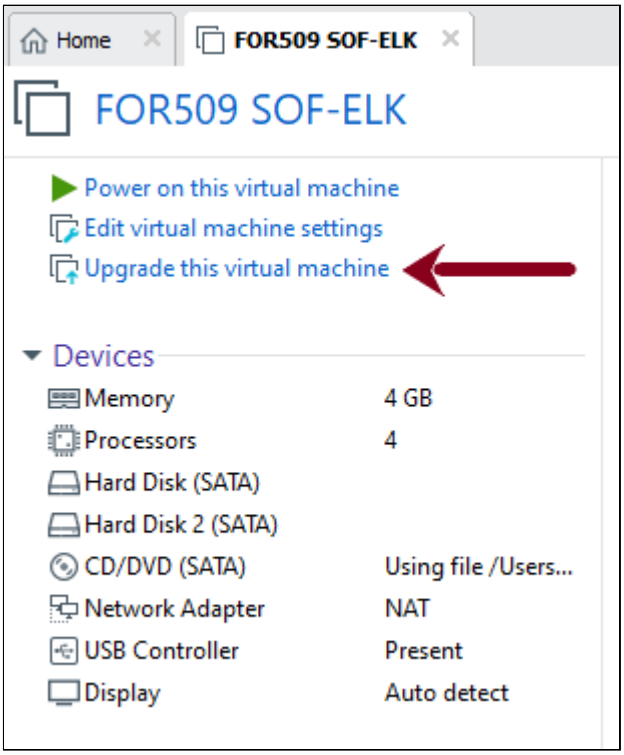
- Start VMWare Workstation or VMWare Player. Select `Open a Virtual Machine`



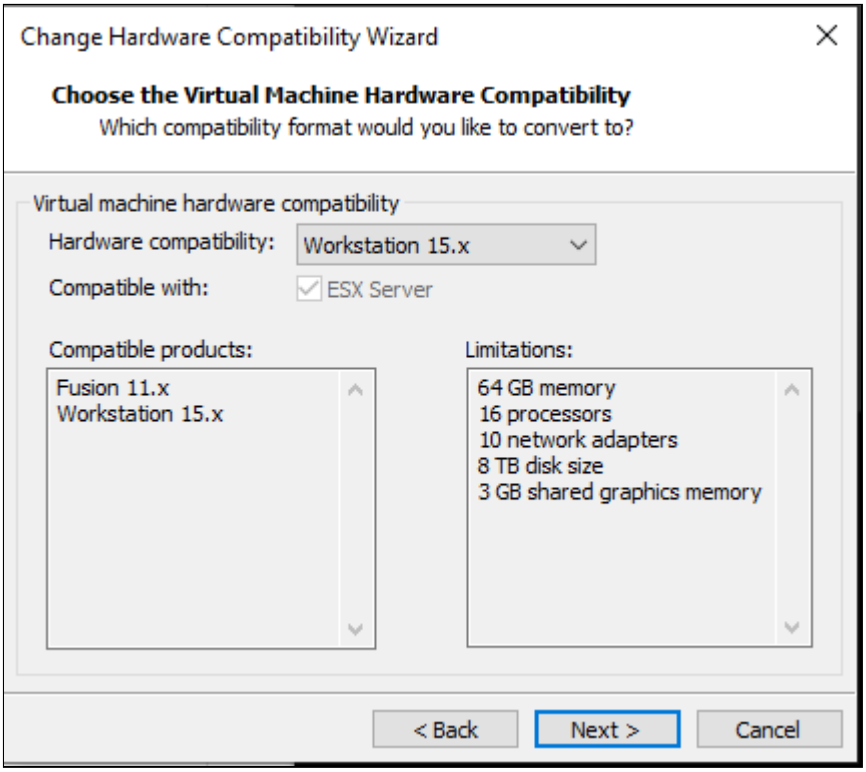
- Navigate to the folder where you previously extracted the files and select `FOR509 SOF-ELK.vmx`



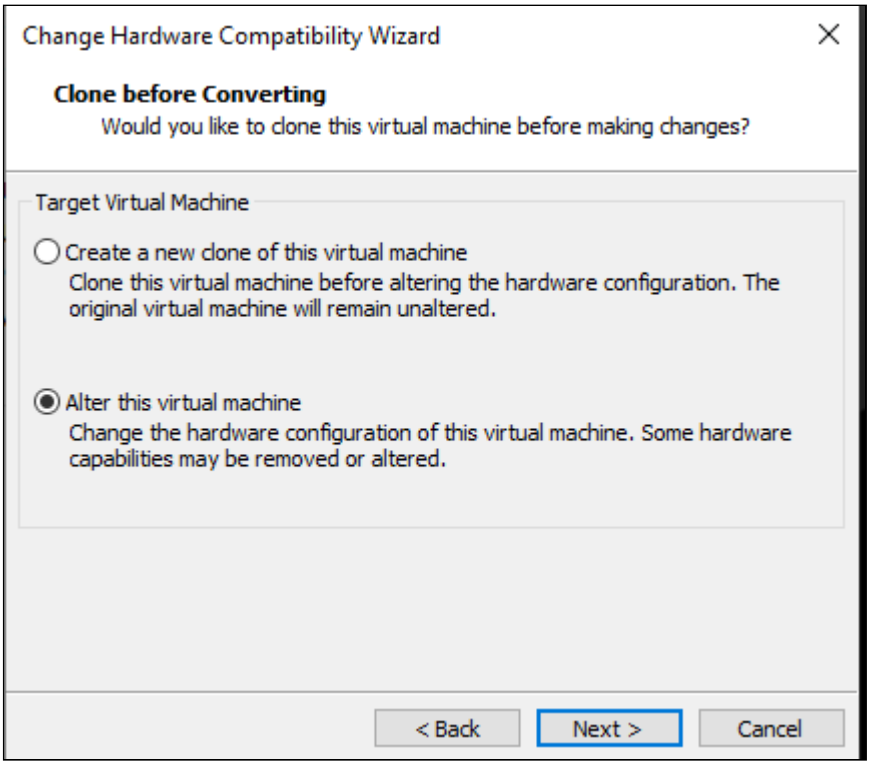
- The FOR509 SOF-ELK virtual machine will open up and you should select `Upgrade this virtual machine`



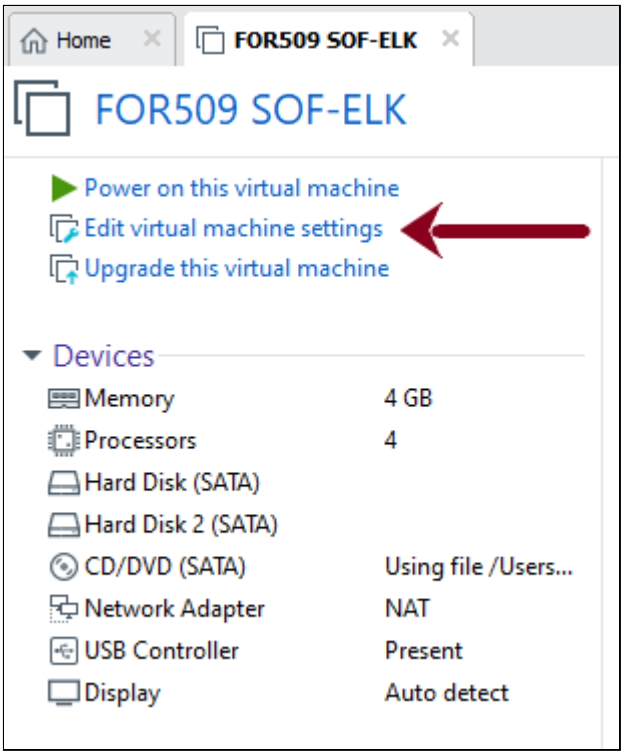
- Select the highest version available under "Hardware compatibility" and click Next



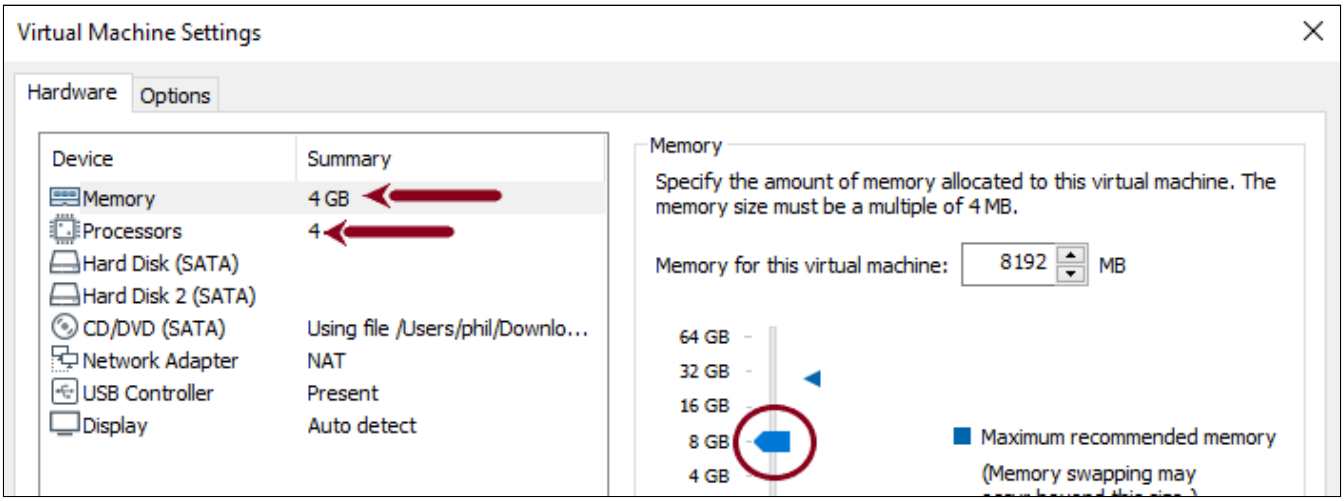
- Select `Alter this virtual machine` and click Next. Click Finish on the next screen



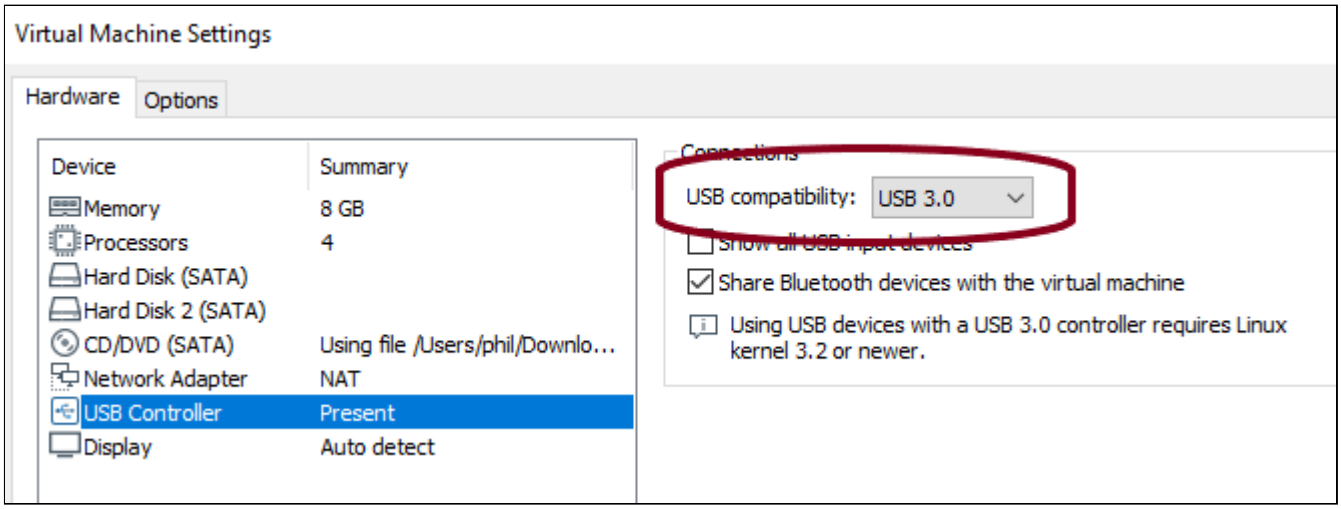
- Next step is to edit the settings



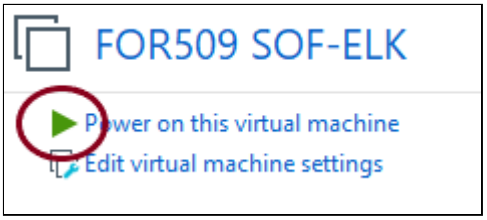
- The ***509 SOF-ELK VM*** requires at least 4GB of RAM. If your host system has more than 8GB of RAM, you can increase the amount of RAM assigned to the virtual machine. The ***509 SOF-ELK VM*** will perform better by giving it more RAM.
- You can also increase the number of processor cores available to the VM. You should assign no more than half the total number of CPU cores available on your host system.



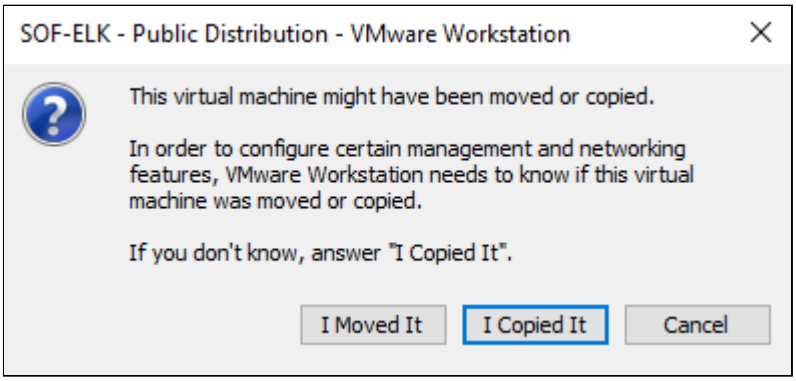
One last thing to check before we start the VM. Make sure the USB settings are set for USB 3.0. Select `USB Controller` and make sure `USB compatibility` is set for `USB 3.0` (select this even if you don't have USB 3.0 on your system as VMWare will still attempt to copy files at a greater speed).



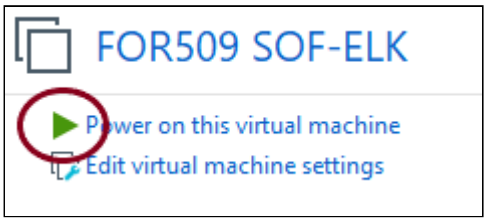
- Select `OK` at the bottom of the settings window. We are ready to start the VM by clicking the green arrow.



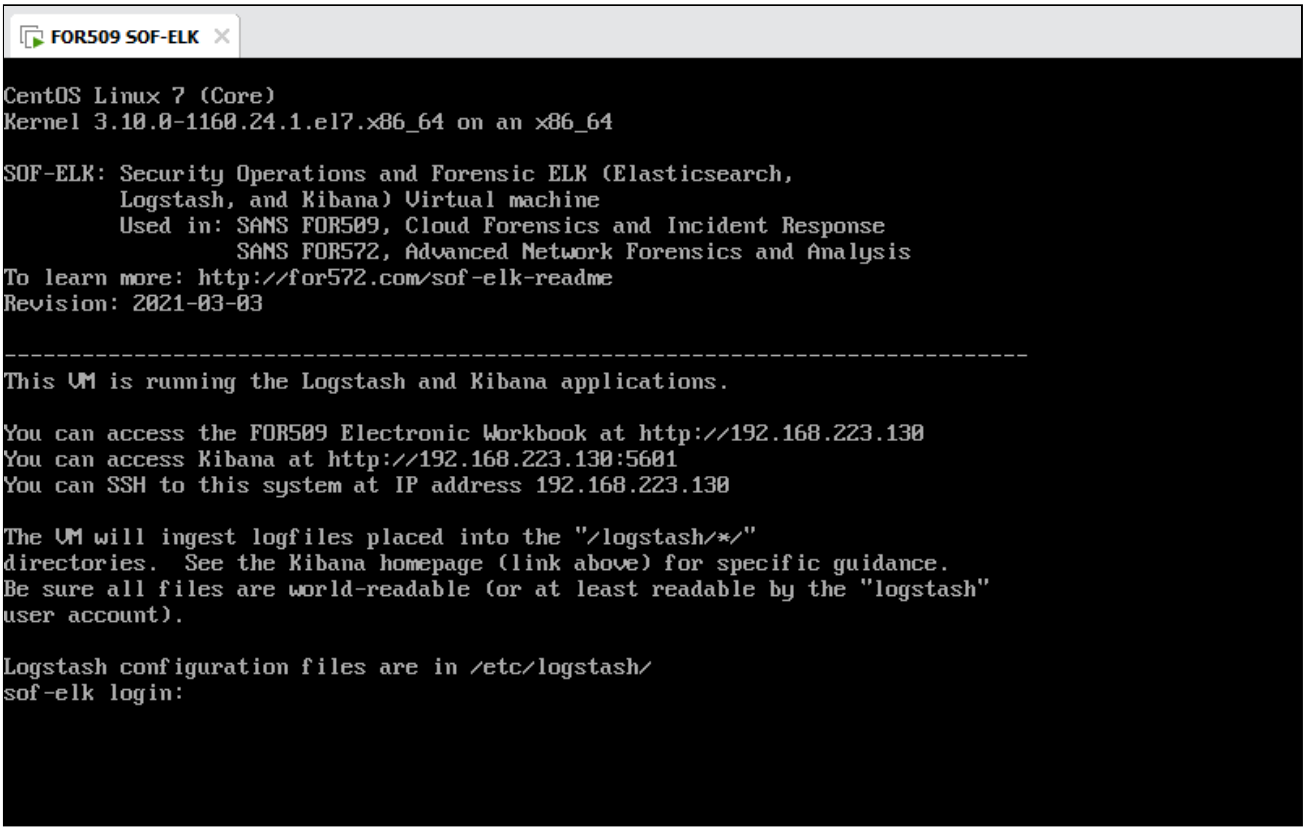
- If prompted whether this machine was moved or copied, choose `I Copied It`



  - If you see any errors regarding `Device or Credential Guard`, you will need to disable Credential Guard or Device Guard. You cannot have two hypervisors running at the same time. See the document: ***Credential Guard / VMWare Workstation Incompatibility Fix***
  - Another error you may encounter is `This host is VT-capable, but VT is disabled`. Most likely VT is disabled in your BIOS and will need to be enbabled.

4. Running the 509 SOF-ELK VM
   -
     If you haven't already done so, start your VM by clicking the green icon 

- Once started, you will see a message showing the IP address of your Kibana instance. While you can login to the machine, this is not necesary. *We will be accessing Kibana via a web browser on your host machine.*



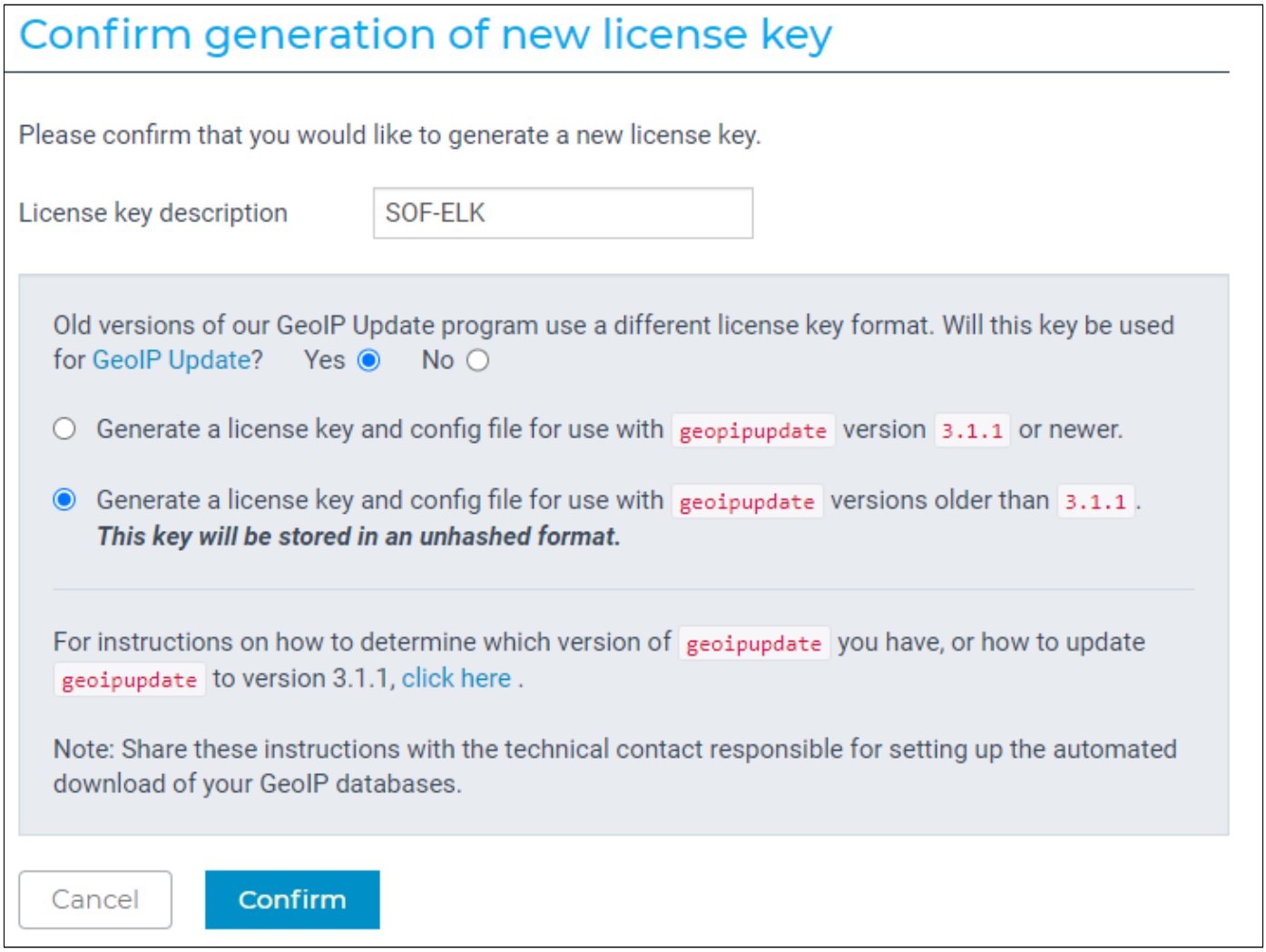
Load MaxMind's GeoIP database

There is great value in being able to geolocate an IP address. Some key information that can be obtained include the country, city, ISP name, and ASN number. Due to licensing restriction we can't pre-load the GeoIP database for you and you will need to complete the following procedure.

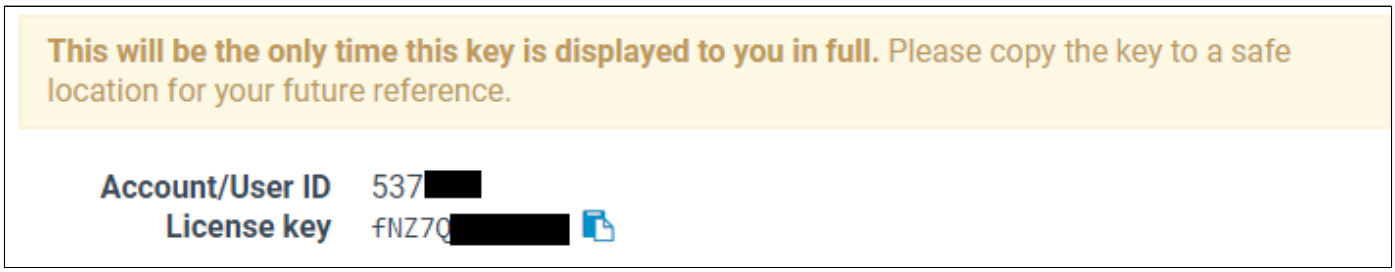
1. Create a free MaxMind account with this link
2. You will receive an email to activate your account and create a password
3. Login to the MaxMind website
4. Select **`Manage License Keys`**

5. Select **`Generate new license key`**

6. Give your key any name you would like and complete the options as shown below



7. Once you select `Confirm` you will get you account number and license key



Be sure to save this information

8. Log on to the SOF-ELK VM with the credentials
    - Username: ***elk_user***
    - Password: ***forensics***

You may log on to the console, however it's recommended to log in via SSH.

9. Enter the command below and provide your account information

```
sudo /usr/local/sbin/geoip_bootstrap.sh
```

```
[elk_user@sof-elk ~]$ sudo /usr/local/sbin/geoip_bootstrap.sh
Do you want to download the MaxMind GeoIP databases?
(This requires free MaxMind account and internet access.)
This prompt will time out in 30 seconds.
Y/N: Y

If you do not already have a MaxMind account, sign up here:
  https://www.maxmind.com/en/geolite2/signup
Once signed in, generate a license key here:
  https://www.maxmind.com/en/accounts/155942/license-key
You have geoipupdate 2.5.0, so ensure you
  create a license key for this version.

Enter your MaxMind Account ID: 537
Enter your MaxMind License Key:
MaxMind GeoIP databases have been installed.
Restarting Logstash to pick up the new database files.

Do you want to set a weekly cron job that will update the MaxMind GeoIP databases automatically?
Y/N: Y
[elk_user@sof-elk ~]$
```

10. If you get an error, retry in a few minutes as it takes a little bit of time for the key to be active
11. You now have a GeoIP database loaded in your SOF-ELK VM which we will use in the next lab

Update SOF-ELK® VM

The SANS team is constantly making improvements to the SOF-ELK VM. To make sure you have the latest configuration and parsers, you will want to run the update script:

```
sudo sof-elk_update.sh
```

If there are no updates, you will get the following result:

```
[elk_user@sof-elk ~]$ sudo sof-elk_update.sh
Up-to-date
[elk_user@sof-elk ~]$
```

If anything has changed, you will see a list of the modified files:

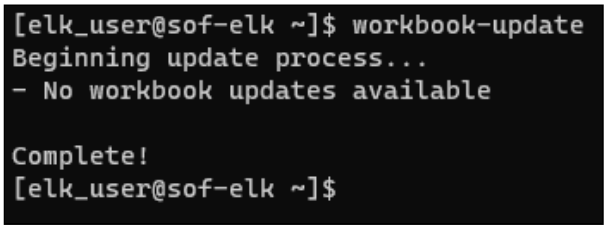
```
[elk_user@sof-elk ~]$ sudo sof-elk_update.sh
[sudo] password for elk_user:
Updating 1990a3f..c197637
Fast-forward
 configfiles/6901-aws.conf         |  1 +
 configfiles/9801-output-aws.conf | 16 ----------------
 2 files changed, 1 insertion(+), 16 deletions(-)
 delete mode 100644 configfiles/9801-output-aws.conf
[elk_user@sof-elk ~]$
```

Updating the E-Workbook

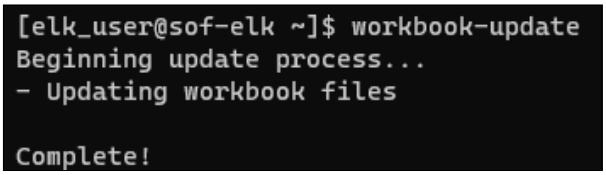
The electronic workbook site is stored locally in the VM so that it is always available. However, course authors may update the source content with minor fixes, such as correcting typos or clarifying explanations, or add new content such as updated bonus labs. You can pull down any available updates into the VM by running the following command:

```
workbook-update
```

If there are no updates, you will get the following result:

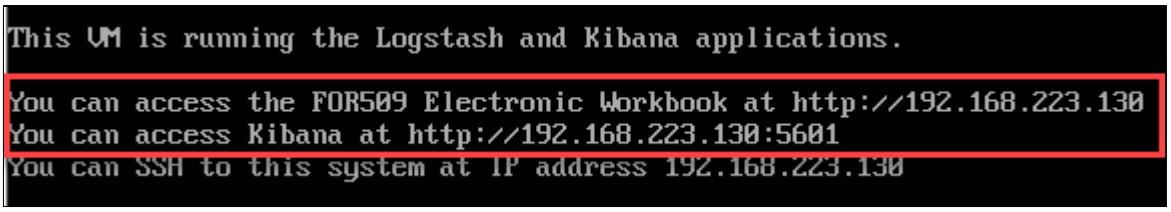


If anything has changed, you will get a messages that the workbook files have been updated:

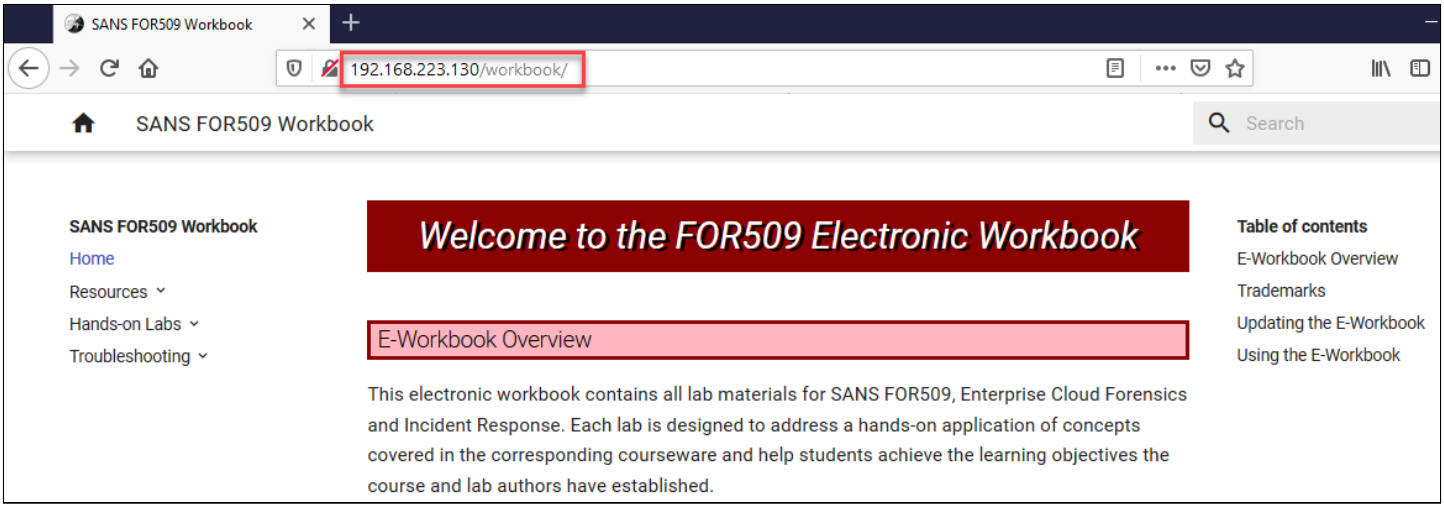


Be sure to refresh any pages you are currently viewing (or restart the browser) to make sure you are seeing the latest content.

Access the E-Workbook and Kibana via your host's web browser

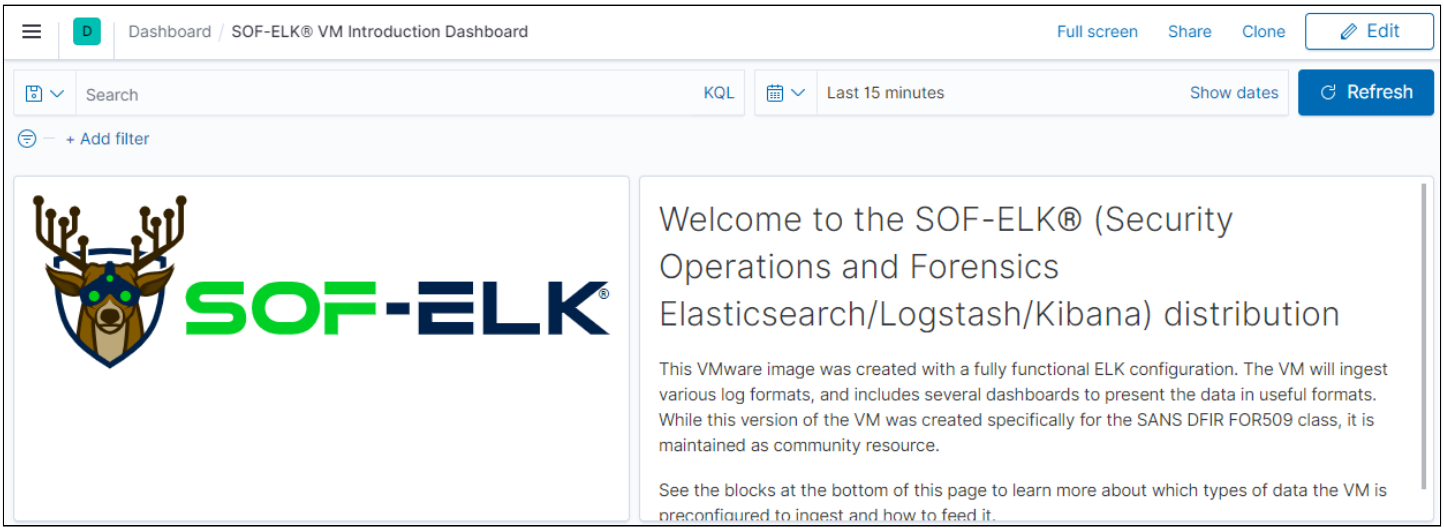


E-Workbook: Using a web browser on your host machine, open the following URL `http://<IP_ADDRESS>/workbook` where the IP is the one displayed in the VMWare console. In this case, it would be `http://192.168.223.130/workbook`



Kibana: Using a web browser on your host machine, open the following URL `http://<IP_ADDRESS>:5601` where the IP is the one displayed in the VMWare console. In this case, it would be `http://192.168.223.130:5601`

You may have to wait a few minutes for Kibana to be ready. Once the page loads, you should see the Kibana default dashboard



Key Takeaways

- You are ready for an exciting week of learning!