Tutorials

A beginner's guide to downloading and getting started with CSI Linux

Before you download the CSI Linux Investigator, you will need to make sure that both Virtual Box and Virtual Box Extensions are installed. If you do not have the Virtual Box Extensions, the Virtual Machines will give you an error when you try to start them.

The minimum requirements for CSI Linux Investigator is at least 8 gigs of ram and 50 gigs of free space on your hard drive to run the virtual machines and 20 gigs of free space for the download.

Now that you have both if the Virtual Box installs complete, you can download the CSI Linux Investigator appliance installer. This is an OVA. file that you can double left click on and Virtual Box should start the process. If you have more than 8 gigs of RAM on your system, we would suggest increasing the CSI Linux Analyst RAM setting to 8,192 instead of 4,096. Make sure the install path is where you want the physical files to reside. Leave the rest as default and finish the wizard install. This will take a few minutes because it is unpacking three operating systems and configuring the environment for you. Once this is complete, you should see three new systems inside Virtual Box which are CSI Linux Analyst, CSI Linux Gateway, and CSI Linux SIEM.

The CSI Linux Analyst is the workhorse that that vast majority of users will spend their time in. Analyst contains the tools for online investigations, traditional computer forensics, malware analysis and threat intelligence. For Dark Web investigations, there are tools for Tor, Freenet, Zeronet, I2P, and crypto currency.

The CSI Linux Gateway is a Tor entry node that can be used by any other virtual machine when configured for it. We use this as an added layer of protection when needed, but it is not required. When you use the gateway in combination with the Analyst, all of the tools and traffic goes through Tor. The benefit is increased anonymity and the ability to use most of the tools with Tor hidden services or .onion domains.

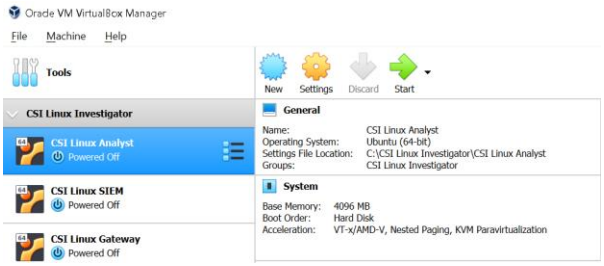
There are two downsides:

1. Going through Tor adds a much longer path to your target on the Internet. This can cause a slight speed decrease.
2. Some websites on the Internet may not trust the Tor exit nodes and may ask you to prove you are not a robot. This may interfere with automated tools and increase false positive and false negative findings. With that said, even without going through Tor, there is always that possibility and it is the job of the investigator to validate their findings.

The CSI Linux SIEM contains Zeek aka bro IDS, Elastic stack, Kibana and some other backend tools. It is managed through a web interface. Like CSI Linux Gateway, it can run separate from the Analyst, but it was designed to work in conjunction with it for onsite live network forensic cases or if you are worried that you're the target of an attack.

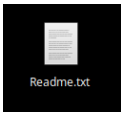
In most cases, CSI Linux Analyst is used as a stand-alone option. We are going to walk through some of the basics of Analyst in this session.

- Double left click on the CSI Linux Analyst icon within Virtual Box. This should start the virtual machine.
- Once the login screen shows up, enter the password "***csi***"
- Press enter or click the "Log In" button.



You should now see the CSI Linux Logo in the background and the task bars on the screen. The task bar on the bottom contains some of the more common tools used for different types of investigations.

- Open the file on the desktop titled "Readme".

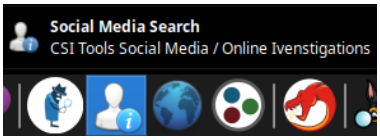


It will explain some of the setup items you will need to look at such as setting up accounts on various site to get your A.P.I. keys along with account information for tools like MISP if they differ from the standard username "***csi***" and password "***csi***.".

The Case folder link on the desktop is where the evidence will be stored. Some of the tools like the Social Media Search and the Domain Information Search will automatically build the case folder and save results into the appropriate case subfolders. You should get in the habit of storing evidence from other tools in the Cases/"***case name***"/export folder or the Cases/"***case name***"/tools folder to keep a standardized repository of your evidence. For example; When you start Autopsy, it is common to save your case file in the tools folder and the exported evidence into the export folder.

When the Social Media Search and the Domain Information Search applications are exited, an MD5 hash of all of the files within the case name folder along with a backed up are then stored in the Cases/Archive folder. Keep in mind that the more evidence you have, the bigger the Virtual Machine disk will need to be which means the more harddrive free space you will need.

Now, to cover some of the tools on the bottom task bar. Let's open The Social Media Search application. We are going to walk through what is happening in the background. You will be asked for a case name. This will be the name of the case you are working on.



- We will call this "***case001***"
- Left click the OK button.

You should be able to see in the case folder window that there are now folders. One is called archive and the next one is called case001 after the case name we just entered. Inside the case001 folder, you should see the common case folders prebuilt for you including the export and tools folder.

We are going to run the username search.

- Make sure it is chosen and left click on OK.
- Enter the username of the target of your investigation.
- Left click on OK.

The tools will start searching for possible user accounts against a list of online websites. Each one that is identified is added to a file starting with Account Search. When the searching is done, you will be asked of you want to open up a browser to list the findings for you to visually verify if the accounts are true positives or false positives. This may take a while since it is opening several new tabs within Google Chrome. Manually go through each finding and visually verify if the account actually exists and if the account is related to the target or suspect. Remove any false positives from the text file and save.

If a twitter account was found, it will gather as much information as it can in the background. When that stage is complete, the Instagram gathering tool will ask for your username and password. This is needed for private information but is not required for public information.

In this example, information was found with the target username.

When the entire process is done, it will ask you foe another username to search for within the same case. If you don't have one:

- Left click on cancel
- Left click OK.

There are several other tools, but for now we will close the case for now.

Let's take a look at what happens when the case is closed. In the main case folder, we will see a file with the case name and an MD5 extension. This contains a hash record of the files created in the case.

We also see an audit log of the tools run within the Social Media Search app.

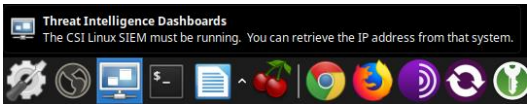
The Domain Information Search tool is very similar. When you run it, it will ask you for a case name and store the data into the "***case name***"/export folder. Let's run the de-cloud application and left click on OK.

It will ask you to enter the domain you want information about. Enter the domain name and left click on OK.

This tool tries to find historical IP addresses associated to the main domain and then does a sub domain search for the top 1 thousand most common sub domains.

Once done, it will show a file with the identified subdomains and ask if you want to open them up in a browser. This will only verify web servers running on port 80. If you want more information, you can use tools like NMAP to run a port scan and see what else is running on domains that exist.

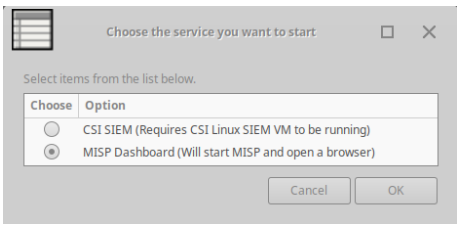
On the bottom left, you should see an icon that looks like a small computer screen.



- Move your mouse over the icon and you will see a description pop up that says "***Threat Intelligence Dashboards***".
- Single left click that icon.

Now, anther screen will pop up that has options for access to the CSI Linux SIEM and MISP. If you had the SIEM running in the background, you would access it through here.

- Left Click on the MISP Dashboard option and left click on OK.



In the background, you will be asked for the password for csi.

- Type csi and press the enter key.

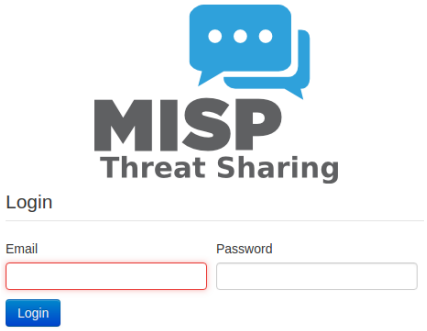
What is happening in the background is that docker is starting up along with the MISP instance. A chrome window should open and this is connecting directly to the MISP.

If this is the first time you have connected to MISP, you may see a certification error claiming that your certificate authority is invalid. This happens because it is using a self-signed certificate. A lot of tools do this.

- Just left click on Advanced.
- Left click on the link that says "***Proceed to localhost (unsafe)***".
- Ignore the warning because you are connecting to local host and there is nothing to intercept since the traffic will not leave the system. Trust the certificate.

Now you should see the MISP log in prompt.

- In the Email field, type "***admin@admin.test***".
- In the Password field, type "***CSILinux.Analyst***".
- Left click Login.



You should now be in the MISP Admin platform.

(MISP has some online training on https://github.com/MISP/misp-training.)

There are a lot more tools located in the top toolbar. Left click on the CSI Linux icon at the top left and you will see sever sub sections

This includes OSINT online investigation and domain reconnaissance options, Secure communication tools, Encryption utilities, Dark Web resources, Incident Response solutions, Computer forensics applications and CSI Tools.

As you can see, there is a lot of power packed into this platform and we have just scratched the surface. Most of the tools have online help or tutorials from the developers or users on Youtube. We will be updating documentation, training, and videos in the future, but there is a lot you can use to get started.

Enjoy the investigation environment and stay tuned for CSI Linux updates and content.

Thank you for using CSI Linux and please give us feedback. We are always trying to improve the product.