IP address identification based on host name

You might need to identify an IP address based on a host name when doing the following:

- Investigating a ransomware attack

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Splunk Enterprise or Splunk Cloud Platform
- System log data

Example

A Windows desktop has been infected by ransomware, and you need to identify the IP address of the infected machine as part of your investigation.

To optimize the search shown below, you should specify an index and a time range.

1. Run the following search:

   <hostname>

2. In the field sections on the left, find and click sourcetype.
3. Click the value with the highest count to add it to the search.
4. In the field sections on the left, find and click src_ip.

Result

This search returns the IP address most likely associated with the host name of the infected machine.