Machine leasing an IP address at a particular time

You might need to discover traffic coming from a particular IP address if you work in a DHCP enabled environment. This procedure allows you to reconcile an IP address to a particular host when IP addresses do not belong to a particular machine.

Required data

**DHCP data**

In addition, this search requires the use of consistent, normalized data provided by the Common Information Model (CIM). This search requires the *Network Sessions data* model. For information on installing and using the CIM, see the Common Information Model documentation.

Procedure

1. Gather the inputs. For example, you might have the IP Address 10.11.36.36 and need to identify the MAC address of the machine that held the lease on January 2nd, 2010 at 9:45AM.
2. Set the search time range to ‘Before’ January 2nd, 2010 at 9:45AM.
3. Run the following search.

```
|datamodel Network_Sessions DHCP search
|search All_Sessions.tag=start All_Sessions.dest_ip=10.11.36.36
|head 1
|table All_Sessions.dest_mac
```

Search explanation

Here is an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

<table>
<thead>
<tr>
<th><strong>Splunk Search</strong></th>
<th><strong>Explanation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>`</td>
<td>datamodel Network_Sessions DHCP search`</td>
</tr>
<tr>
<td>`</td>
<td>search All_Sessions.tag=start All_Sessions.dest_ip=10.11.36.36`</td>
</tr>
</tbody>
</table>
### Splunk Search

<table>
<thead>
<tr>
<th>head 1</th>
</tr>
</thead>
</table>

| table All_Sessions.dest_mac |

### Explanation

10.11.36.36.

Limit the data returned to the first result.

Display the MAC address from the event in

### Next steps

This search returns a MAC address that identifies the machine that was leasing the IP address at the specified time. After you have identified the MAC address, these are some possible next steps:

- If the user is identifiable based on the MAC address, communicate with the user.
- If the user is not identifiable by the MAC address, [investigate the MAC address](#) to determine who owns it.

Finally, you might be interested in other processes associated with the [Processing DMCA notices](#) use case.