Removable devices connected to a machine

You might need to identify removable devices that were connected to computer or other network device 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 that you believe might have been transmitted through a USB drive. You want to identify the drive.

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

1. Run the following search:
   
   ```
   sourcetype=winregistry friendlyname
   ```

2. Expand a result and look at the registry_value_data field.

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>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourcetype=winregistry</td>
<td>Search only Windows Registry logs.</td>
</tr>
<tr>
<td>friendlyname</td>
<td>Search for a registry entry value specific to USB</td>
</tr>
</tbody>
</table>
### Splunk Search | Explanation

- devices. If friendlyname doesn’t yield results, try other entries, as described in [Microsoft documentation](#).

---

**Result**

The value in the registry_value_data field is the name of the USB device. After you have identified the device, you might want to look at the host or src_ip fields in the search result to identify the machine the device was plugged into. You might also want to identify any files that were downloaded from the removable device.