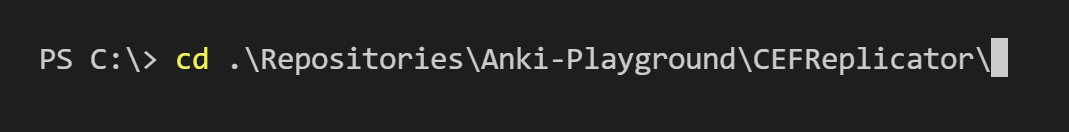
**How to use it:**

Unzip the CEFReplicator.zip and you must see the files below

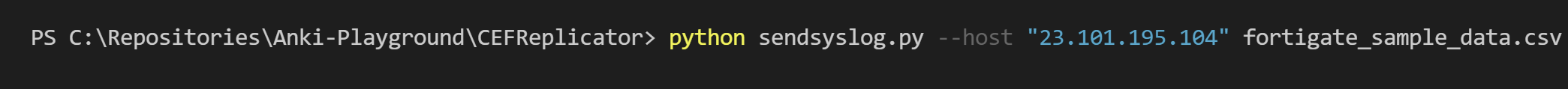
Table

Description automatically generated with medium confidence

Navigate to this folder, for example



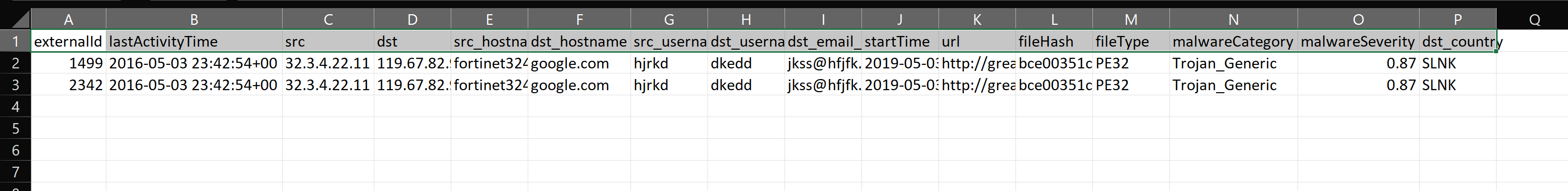
Run the python utility (sendsyslog.py) like shown below



About the Utility:

**CEFReplicator** - This utility helps to replay CEF events. Sample events need to be stored into a file in csv format and file name will be provided as an argument on to this utility.

Sample file structured as header and followed by data, (you can see below)

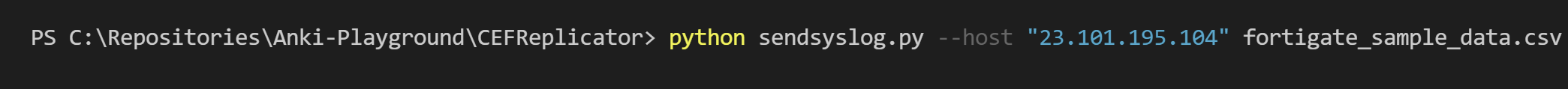


Make sure you will provide valid file as input.

1. First row will be considered as header always, so make sure you will have header only at the beginning
2. Make sure at least 1 record present after header, if no events present then we take default sample event (hard coded)
3. If you don’t provide valid file, then this utility will generate sample event with default event

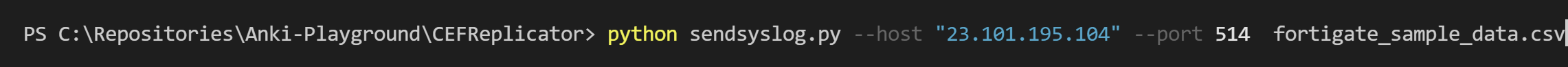
Sample invocations:

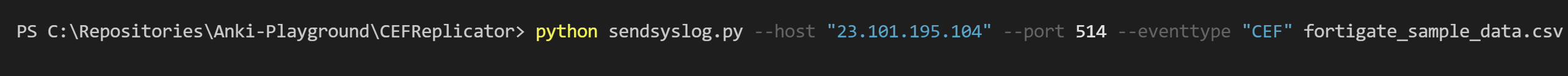
“--host” is and sample file name are mandatory. Make sure to provide these 2

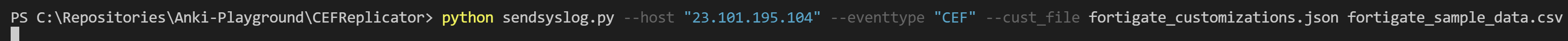


By default it generates 100 times to the sample data and provide the inputs “--eps” if you need more

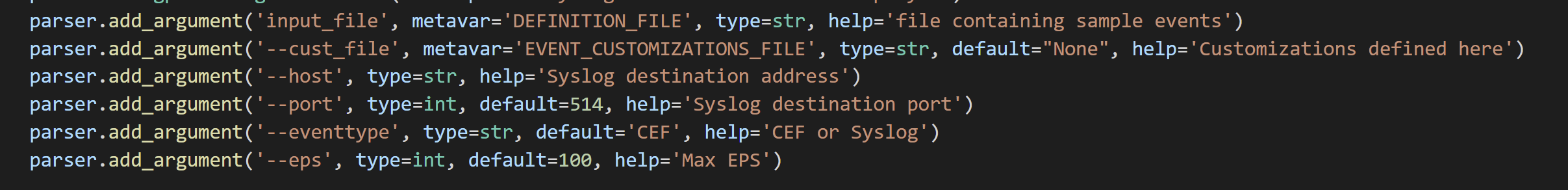






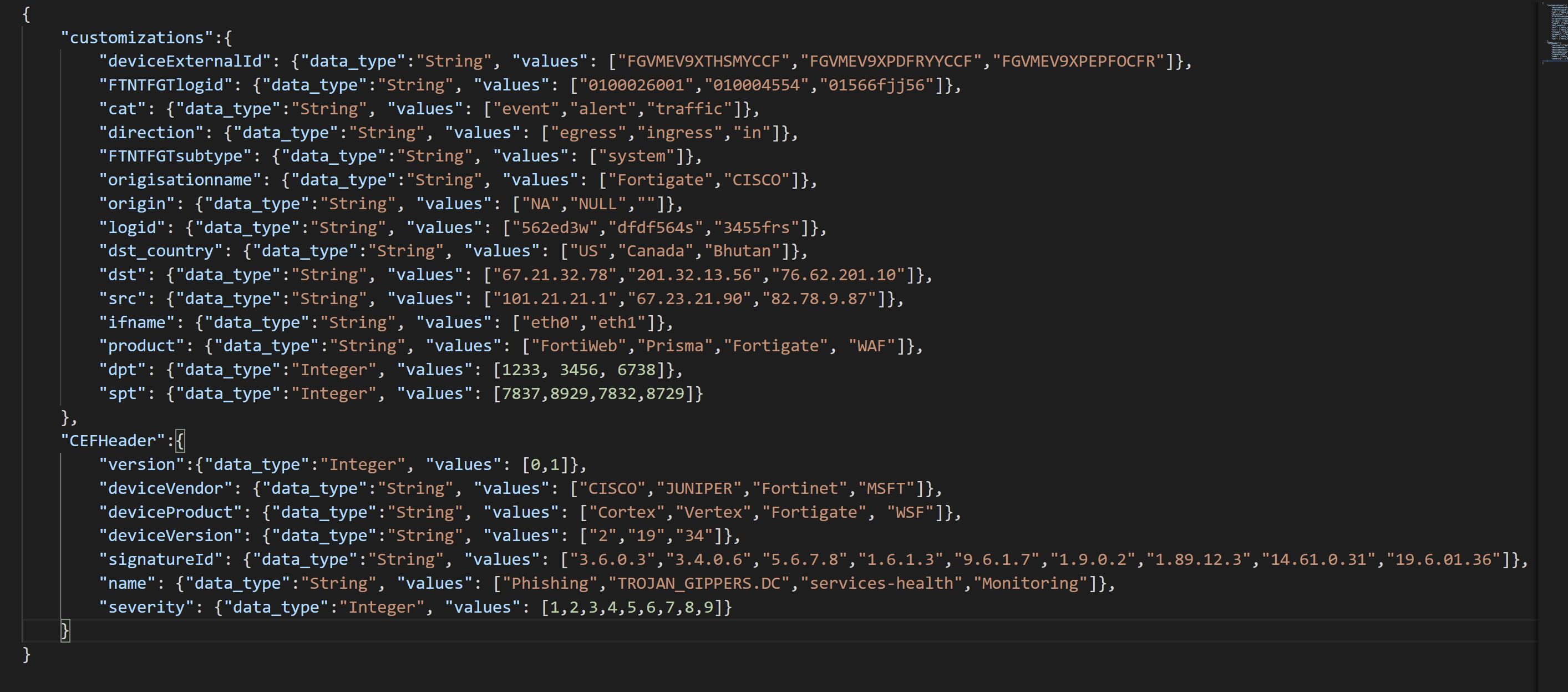


Here is the complete list of other arguments

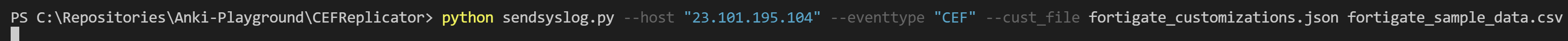


If you would need to prepare CEF event with any customizations (other than sample event), we must specify customization requirements in a specific schema and this file name also need to be passed as an argument.

For example, see below how the customization defiled –



Store above customizations into a json file as pass file name as an argument (--cust\_file) as shown below



When we have customizations defined, field values from sample events will be replaced by the custom values that are defined in this section.

**Visualizing events:**

A screenshot of a computer

Description automatically generated with medium confidence

Troubleshooting:

If you are not running this utility where we have LA agent installed, then follow below steps that are described at –

[CEF & Syslog Step by Step Troubleshooter - Overview (azure.com)](https://dev.azure.com/SupportabilityWork/Azure%20Security/_wiki/wikis/Azure%20Sentinel%20CSS%20wiki/3822/CEF-Syslog-Step-by-Step-Troubleshooter)

[Syslog Workflow - ASA, Check Point, Syslog, Palo Alto, Fortigate, Cisco, CEF - Overview (azure.com)](https://dev.azure.com/SupportabilityWork/Azure%20Security/_wiki/wikis/Azure%20Sentinel%20CSS%20wiki/1345/Syslog-Workflow-ASA-Check-Point-Syslog-Palo-Alto-Fortigate-Cisco-CEF)

If you are running locally (where we have LA forwarder installed) then you may not require to validate remote communication part of it, check other troubleshooting steps