**How to use it:**

Unzip the CEFReplicator.zip on to the system that is designated to generate syslog traffic. This can be on the same system where LA Agent is setup and running or on a separate system.

You will see the files like shown below.

Table

Description automatically generated with medium confidence

We have 2 flavors / variants

1. Generating syslog / cef traffic from raw log
2. Generating syslog / cef traffic from csv file

**Generating syslog / cef traffic from raw log**

Step 1: Make sure raw log present in a file (with any extension) and each record separated by new line char (\n)

For example:

Inflobox NIOS raw logs:

*May 13 2022 12:05:52 10.0.0.0 dhcpd[30174]: DHCPDISCOVER from 0a:0b:0c:0d::0f via eth2 TransID 5daf9374: network 10.0.0.0/24: no free leases*

*May 13 2022 12:05:52 10.1.1.1 named[11325]: zone voip.abc.com/IN: ZRQ applied transaction 0101010 with SOA serial 9191919. Zone version is now 0202020.*

*May 13 2022 12:05:52 10.0.0.0 dhcpd[30174]: DHCPDISCOVER from 0a:0b:0c:0d::0f via eth2 TransID 5daf9374: network 10.0.0.0/24: no free leases*

*May 13 2022 12:05:52 10.1.1.1 named[11325]: zone voip.abc.com/IN: ZRQ applied transaction 0101010 with SOA serial 9191919. Zone version is now 0202020.*

CISCO Meraki raw logs:

*1377449842.514782056 MX84 ids-alerts : signature=129:4:1 priority=3 timestamp=1377449842.512569 direction=ingress protocol=tcp/ip src=74.125.140.132:80*

*1380664994.337961231 MX84 events : type=vpn\_connectivity\_change vpn\_type='site-to-site' peer\_contact='98.68.191.209:51856' peer\_ident='2814ee002c075181bb1b7478ee073860' connectivity='true'*

*1377448470.246576346 MX84 ids-alerts : signature=119:15:1 priority=2 timestamp=1377448470.238064 direction=egress protocol=tcp/ip src=192.168.111.254:56240 signature=1:28423:1 priority=1 timestamp=1468531589.810079 dhost=98:5A:EB:E1:81:2F direction=ingress protocol=tcp/ip src=151.101.52.238:80 dst=192.168.128.2:53023 message: EXPLOIT-KIT Multiple exploit kit single digit exe detection url=http://www.eicar.org/download/eicar.com.txt src=192.168.128.2:53150 dst=188.40.238.250:80 mac=98:5A:EB:E1:81:2F name='EICAR:EICAR\_Test\_file\_not\_a\_virus-tpd'// 1563249630.774247467 remote\_DC1\_appliance security\_event ids\_alerted signature=1:41944:2 priority=1 timestamp=TIMESTAMPEPOCH.647461 dhost=74:86:7A:D9:D7:AA direction=ingress protocol=tcp/ip src=23.6.199.123:80 dst=10.1.10.51:56938 message: BROWSER-IE Microsoft Edge scripting engine security bypass css attempt*

*1380653443.857790533 MR18 events : type=device\_packet\_flood radio='0' state='end' alarm\_id='4' reason='left\_channel' airmarshal\_events type= rogue\_ssid\_detected ssid='' bssid='02:18:5A:AE:56:00' src='02:18:5A:AE:56:00' dst='02:18:6A:13:09:D0' wired\_mac='00:18:0A:AE:56:00' vlan\_id='0' channel='157' rssi='21' fc\_type='0' fc\_subtype='5'*

*1380653443.857790533 MS220\_8P events : type=8021x\_eap\_success port='' identity='employee@ikarem.com'*

*1374543213.342705328 MX84 urls : src=192.168.1.186:63735 dst=69.58.188.40:80 mac=58:1F:AA:CE:61:F2 request: GET https://...*

*1374543986.038687615 MX84 flows : src=192.168.1.186 dst=8.8.8.8 mac=58:1F:AA:CE:61:F2 protocol=udp sport=55719 dport=53 pattern: allow all*

Step 2: Save in same folder as script exist, name and extension can be any thing

Step 3: Navigate to the script path, where *syslogfromraw.py* exists

For example, if script exists in C:\Repositories\Anki-Playground\CEFReplicator then run

c*d C:\Repositories\Anki-Playground\CEFReplicator*

Step 4: You can try with the following commands

1. *python syslogfromraw.py --host "13.87.202.58" --port 514 --eventtype 'syslog' --cust\_file fortigate\_customizations.json syslog\_meraki\_raw.log*
2. *python syslogfromraw.py --host "13.87.202.58" --port 514 --eventtype 'syslog' syslog\_meraki\_raw.log*
3. *python syslogfromraw.py --host "13.87.202.58" --port 514 --eventtype 'cef' --cust\_file fortigate\_customizations.json cef\_microsoft\_ata.log*
4. *python syslogfromraw.py --host "13.87.202.58" --port 514 --eventtype 'cef' cef\_microsoft\_ata.log*

**arguments*:***

--cust\_file (optional – Name of the file where we have customizations defined)

--port (optional – default is 514 if not specified)

--host (optional – default is localhost if not specified)

--eventtype (optional – default is cef if not specified)

--eps (optional – default is 100 if not specified)

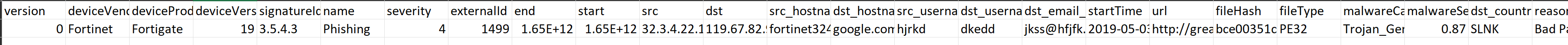
**Name of the file where we have same data is mandatory like** *python syslogfromcsv.py cef\_microsoft\_ata.log*

**Generating syslog / cef traffic from csv filelog**

Step 1: Make sure csv file present with header and at least 1 record, records are separated by new line char (\n)

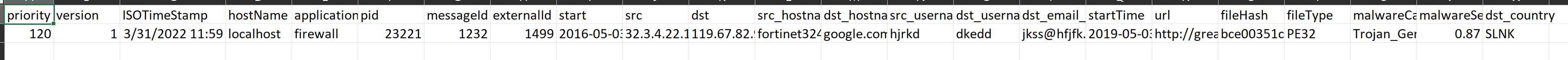
For example:

FortiGate sample data in syslog converted into csv:



Note: Make sure header fields also exist in csv along with the structured data

FortiGate sample data in syslog converted into csv:

**

Step 2: Save in same folder as script exist, name and extension can be any thing

Step 3: Navigate to the script path, where *syslogfromraw.py* exists

For example, if script exists in C:\Repositories\Anki-Playground\CEFReplicator then run

c*d C:\Repositories\Anki-Playground\CEFReplicator*

Step 4: You can try with the following commands

1. *python syslogfromcsv.py --host "13.87.202.58" --port 514 --eventtype 'syslog' --cust\_file 'fortigate\_customizations.json' syslog\_fortigate\_sample\_data.csv*
2. *python syslogfromcsv.py --host "13.87.202.58" --port 514 --eventtype 'syslog' syslog\_fortigate\_sample\_data.csv*
3. *python syslogfromcsv.py --host "13.87.202.58" --port 514 --eventtype ‘cef’ --cust\_file 'fortigate\_customizations.json' cef\_fortigate\_sample\_data.csv*
4. *python syslogfromcsv.py --host "13.87.202.58" --port 514 --eventtype ‘cef’ cef\_fortigate\_sample\_data.csv*

**arguments*:***

--cust\_file (optional – Name of the file where we have customizations defined)

--port (optional – default is 514 if not specified)

--host (optional – default is localhost if not specified)

--eventtype (optional – default is cef if not specified)

--eps (optional – default is 100 if not specified)

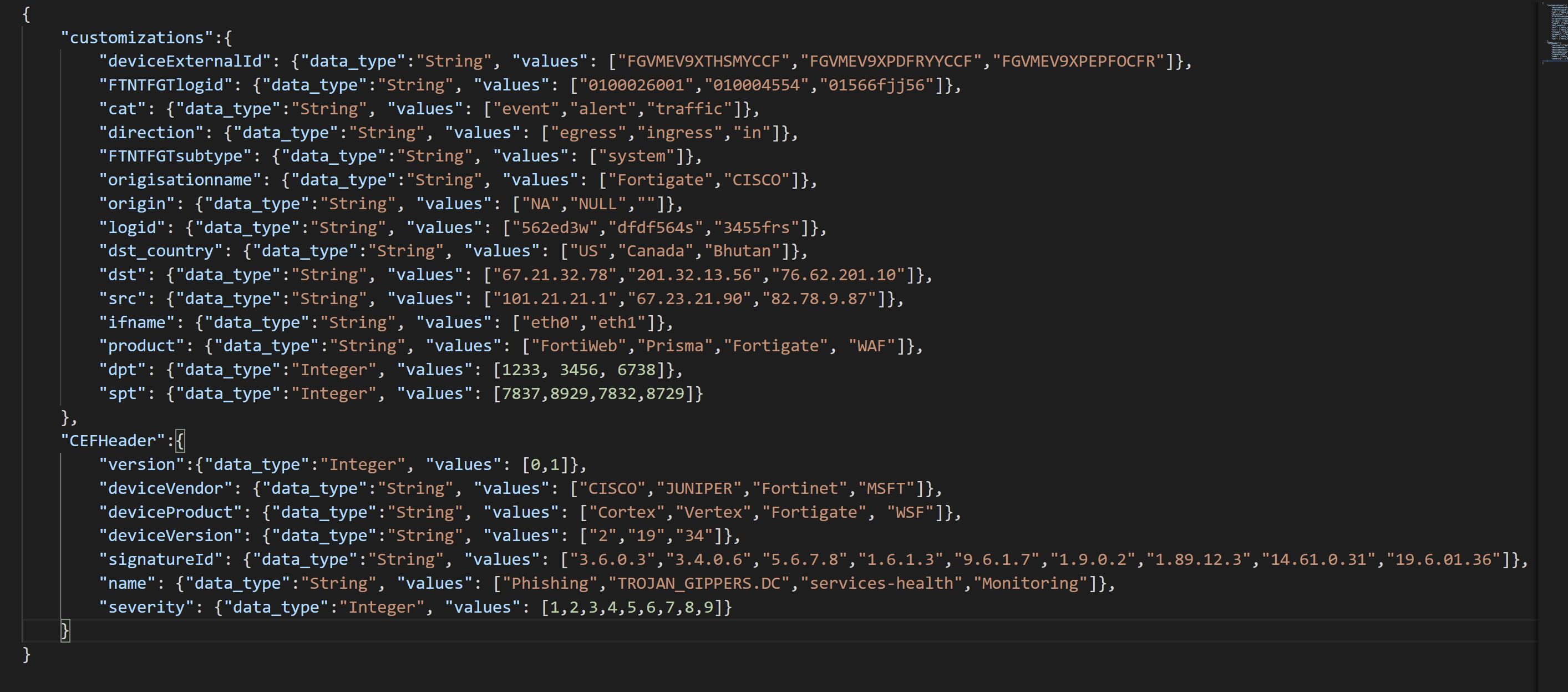
**Name of the file where we have same data is mandatory like** *python syslogfromcsv.py cef\_fortigate\_sample\_data.csv*

Additional information:

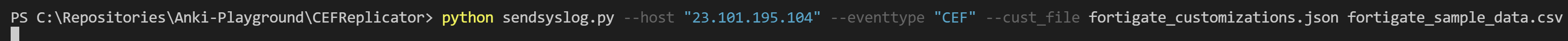
**Log customizations:**

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