Fixit

Fixit Challenge

In this challenge room, you will act as John, who has recently cleared his third screening interview for the SOC-L2 position at MSSP Cybertees Ltd, and a final challenge is ready to test your knowledge, where you will be required to apply the knowledge to FIX the problems in Splunk.
You are presented with a Splunk Instance and the network logs being ingested from an unknown device.

Pre-requisites

This challenge is based on the knowledge covered in the following rooms:

- Regex
- Splunk: Exploring SPL
- Splunk: Data Manipulation

Room Machine

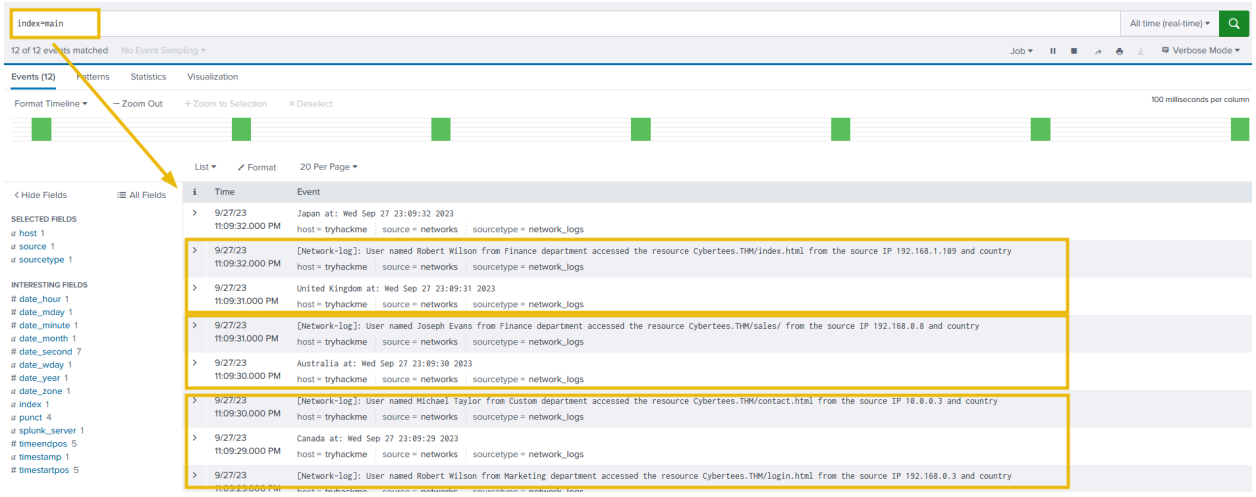
Before moving forward, start the lab by clicking the Start Machine button. The lab will be accessible via split screen. If the VM is not visible, use the blue Show Split View button at the top-right of the page. Once the VM is in split screen view, you can click the + button to show it on a full screen. The VM will take 3-5 minutes to load properly. In this room, we will be working using the terminal of the VM and accessing the Splunk instance at MACHINE_IP:8000.
Note: Splunk is installed in the /opt/splunk directory, and you will be working in the App called Fixit.

Challenge: FIXIT

This challenge is divided into three levels:

Level 1: Fix Event Boundaries

Fix the Event Boundaries in Splunk. As the image below shows, Splunk cannot determine the Event boundaries, as the events are coming from an unknown device.



Level 2: Extract Custom Fields

Once the event boundaries are defined, it is time to extract the custom fields to make the events searchable.

- Username
- Country
- Source_IP
- Department
- Domain

Sample Logs:

To create regex patterns, sample Network logs are shown below:

```
[Network-log]: User named Johny Bil from Development department accessed the resource Cybertees.THM/about.html from the source IP 192.168.0.1 and country
Japan at: Thu Sep 28 00:13:46 2023
[Network-log]: User named Johny Bil from Marketing department accessed the resource Cybertees.THM/about.html from the source IP 192.168.2.2 and country
Japan at: Thu Sep 28 00:13:46 2023
[Network-log]: User named Johny Bil from HR department accessed the resource Cybertees.THM/about.html from the source IP 10.0.0.3 and country

Japan at: Thu Sep 28 00:13:46 2023
```

Level 3: Perform Analysis on the FIXED Events

Once the custom fields are parsed, we can use those fields to analyze the Event logs. Examine the events and answer the questions.

Happy Fixing!

****

Answer the questions below:

What is the full path of the FIXIT app directory?

```
ubuntu@tryhackme:/opt/splunk/etc/apps$ ls
SplunkForwarder                 splunk-dashboard-studio
SplunkLightForwarder            splunk_archiver
alert_logevent                  splunk_assist
alert_webhook                   splunk_essentials_9_0
appsbrowser                     splunk_gdi
fixit                           splunk_httpinput
introspection_generator_addon   splunk_instrumentation
journald_input                  splunk_internal_metrics
launcher                        splunk_metrics_workspace
learned                         splunk_monitoring_console
legacy                          splunk_rapid_diag
python_upgrade_readiness_app    splunk_secure_gateway
sample_app                      user-prefs
search
```

Answer: /opt/splunk/etc/apps/fixit

What Stanza will we use to define Event Boundary in this multi-line Event case?
The answer to this one was found in the notes related to the Splunk: Data Manipulation room that was a prerequisite for this one.
Answer: BREAK_ONLY_BEFORE

In the inputs.conf, what is the full path of the network-logs script?

```
root@tryhackme:/opt/splunk/etc/apps/fixit/default# cat inputs.conf
[script:///opt/splunk/etc/apps/fixit/bin/network-logs]

index = main
source = networks
sourcetype = network_logs
interval = 1
```

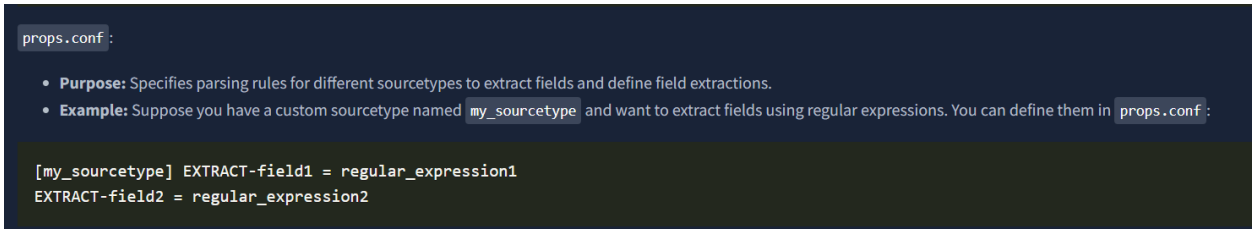
Answer: /opt/splunk/etc/apps/fixit/bin/network-logs

What regex pattern will help us define the Event's start?

Our source type is the network logs so the events start with the network logs.
Answer: \[Network-log\]

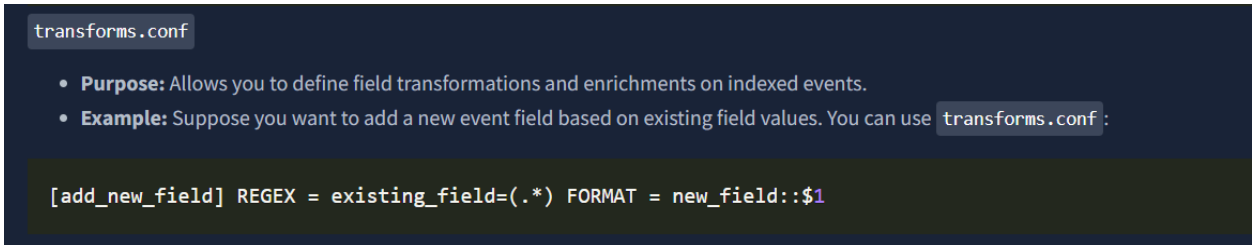
What is the captured domain?
We need to create a few more configuration files for the Fixit app to work.

First, I need to create a props.conf file.

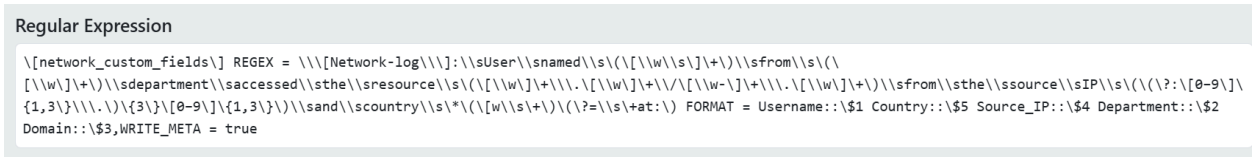



```
root@tryhackme:/opt/splunk/etc/apps/fixit/default# nano props.conf
root@tryhackme:/opt/splunk/etc/apps/fixit/default# cat props.conf
[network_logs]
SHOULD_LINEMERGE =true
BREAK_ONLY_BEFORE = \[Network-log\]
TRANSFORM-network = network_custom_fields
```

Next, we need transforms.conf.



To create the transforms.conf file I'll need to create a regex for the sample network logs provided above. To do this I used https://regex-generator.olafneumann.org/ and pasted the sample logs. This gave me the following regex.



Using this regex to create the transforms.conf file leaves us with the following:

```
root@tryhackme:/opt/splunk/etc/apps/fixit/default# nano transforms.conf
root@tryhackme:/opt/splunk/etc/apps/fixit/default# cat transforms.conf
[network_custom_fields]
REGEX = \[Network-log\]:\sUser\snamed\s([\w\s]+)\sfrom\s([\w]+)\sdepartment\saccessed\sthe\sresource\s([\w]+\.[\w]+\/[\w-]+\.[\w]+)\sfrom\sthe\ssource\sIP\s((?:[0-9]{1,3
}\.){3}[0-9]{1,3})\sand\scountry\s*([w\s+)(?=\s+at:)
FORMAT = Username::$1 Country::$5 Source_IP::$4 Department::$2 Domain::$3,WRITE_META = true
```

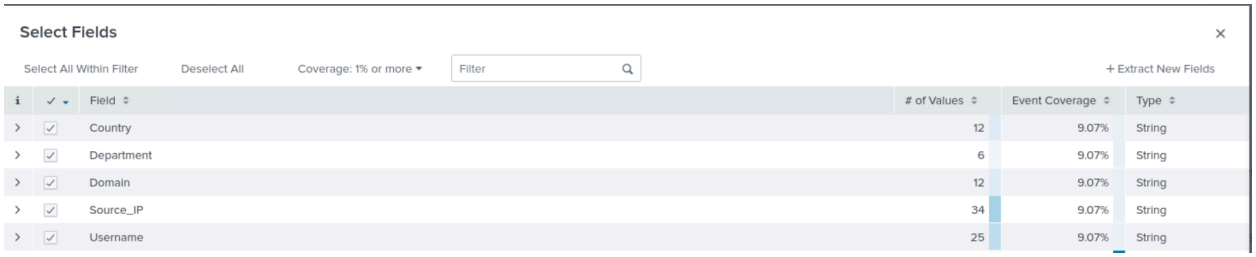
Finally, the fields.conf file. This one is straightforward, I just need a field for each piece of information filtered out by our regular expression.

```
root@tryhackme:/opt/splunk/etc/apps/fixit/default# nano fields.conf
root@tryhackme:/opt/splunk/etc/apps/fixit/default# cat fields.conf
[Username]
INDEXED = true

[Country]
INDEXED = true

[Source IP]
INDEXED = true

[Department]
INDEXED = true

[Domain]
INDEXED = true
```

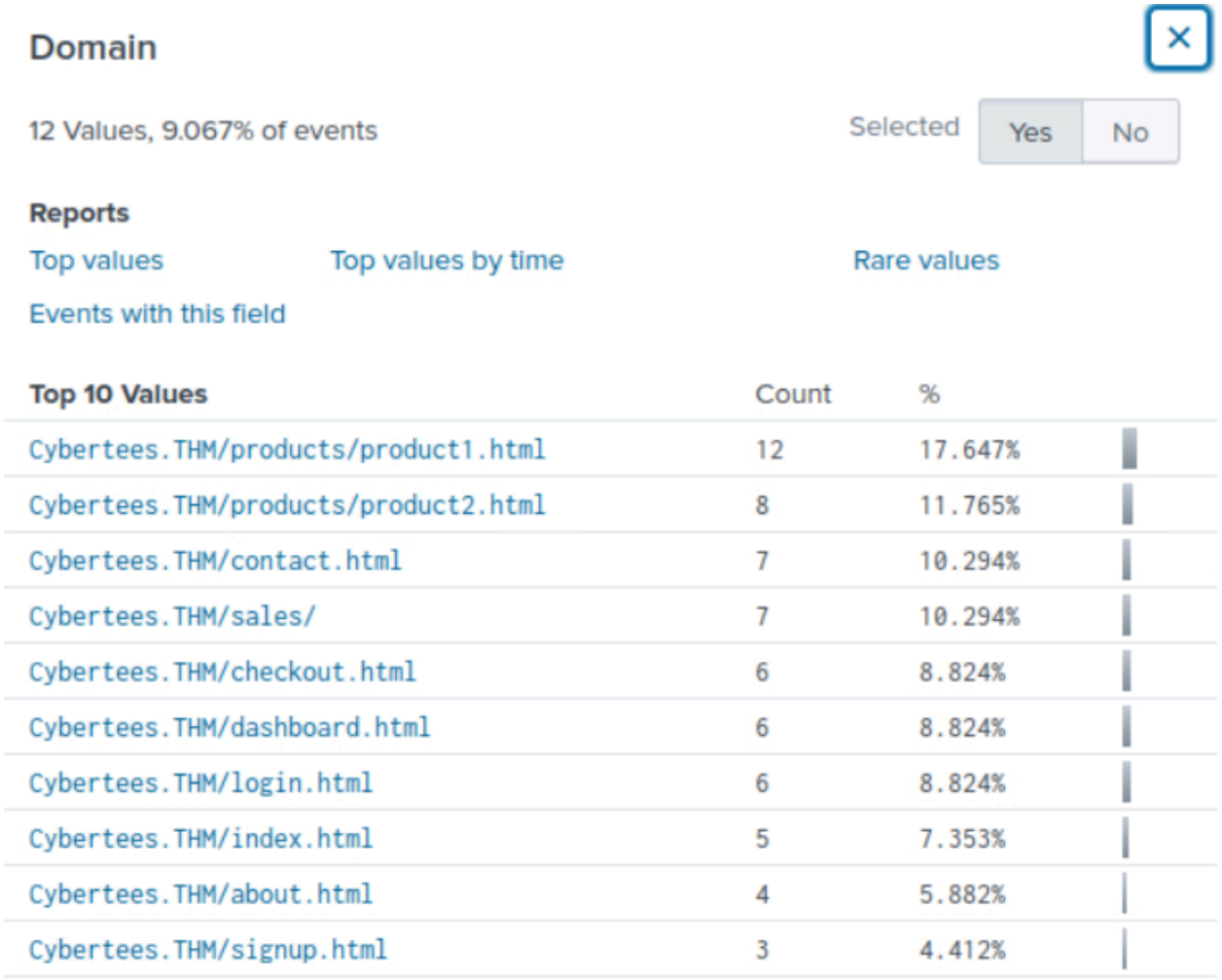
Now, after restarting Splunk by running the following command:

```
root@tryhackme:/opt/splunk/bin# ./splunk restart
```

We will see the five fields we added.

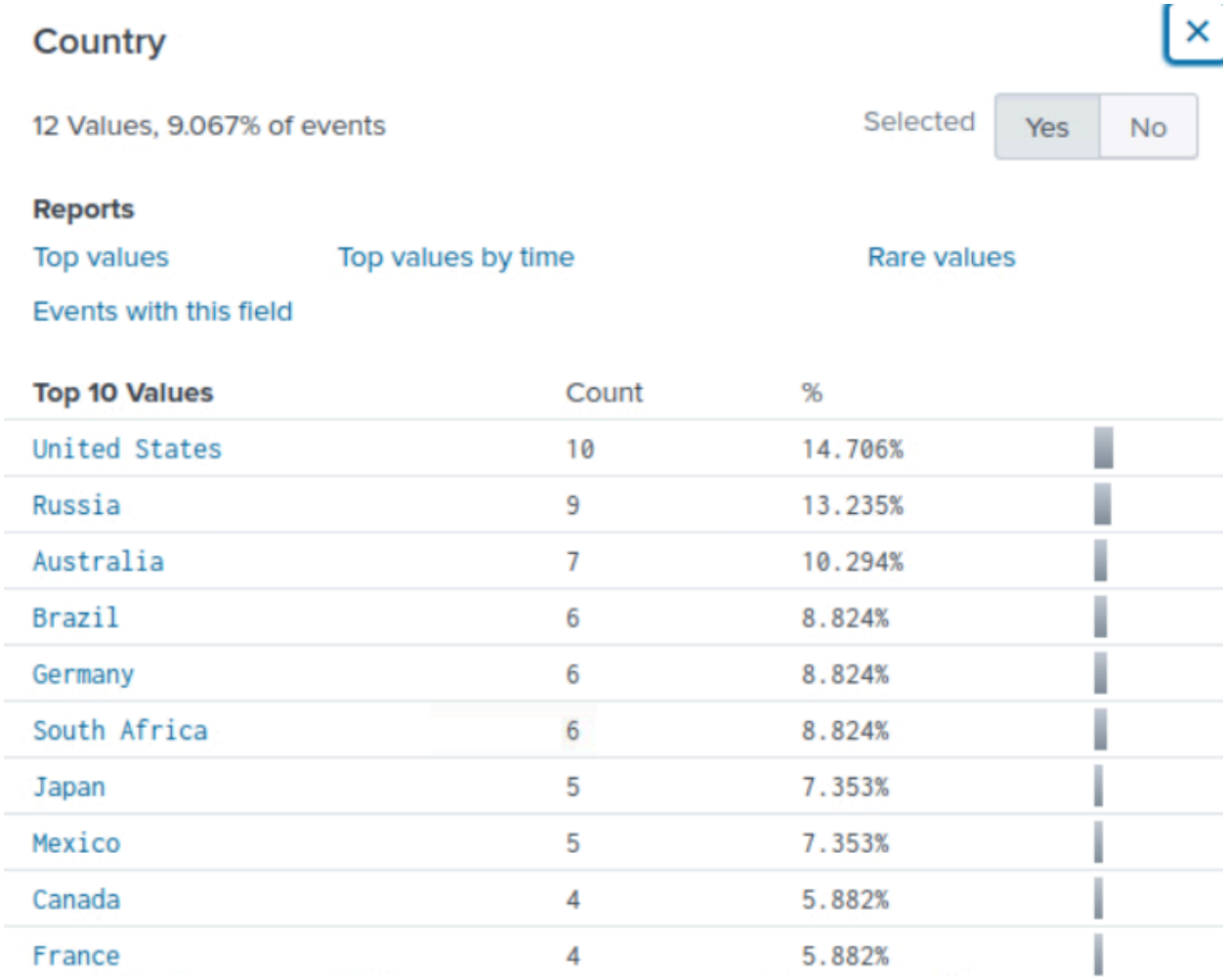


Now for the domain in question:



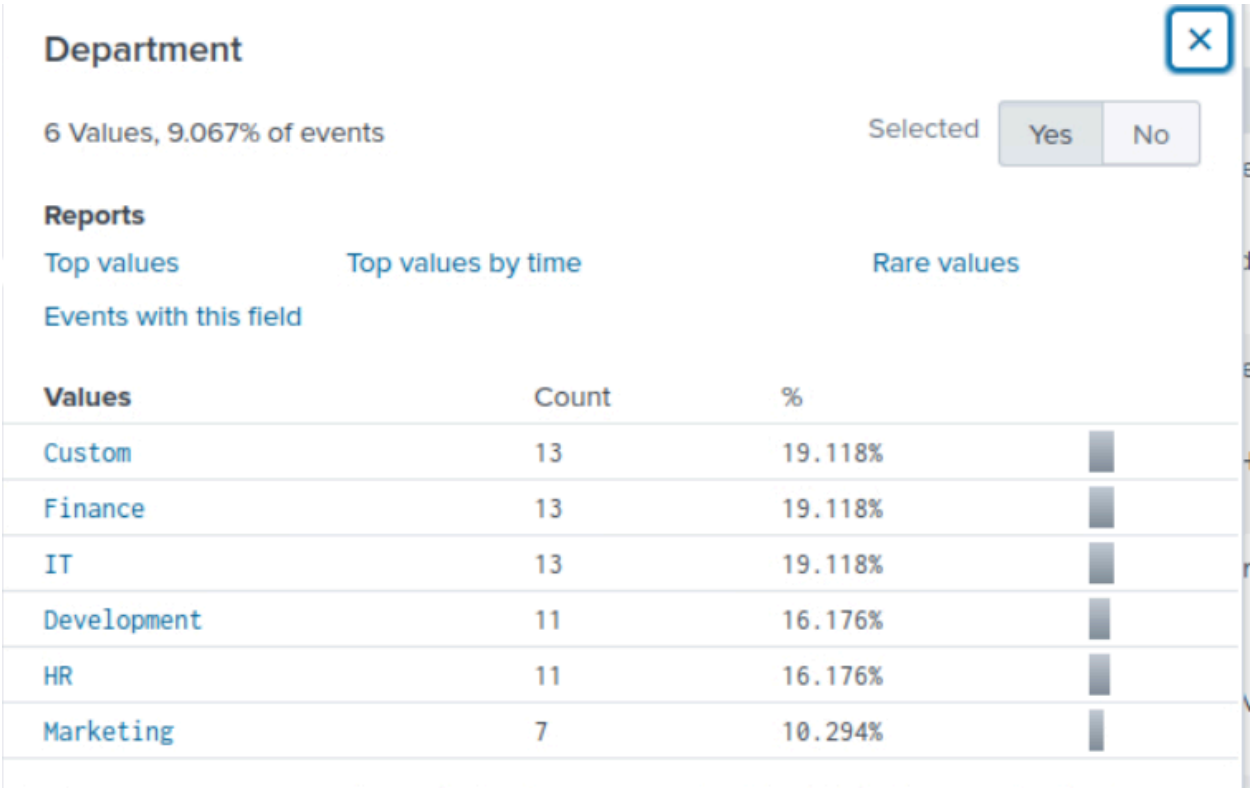
Answer: Cybertees.THM

How many countries are captured in the logs?



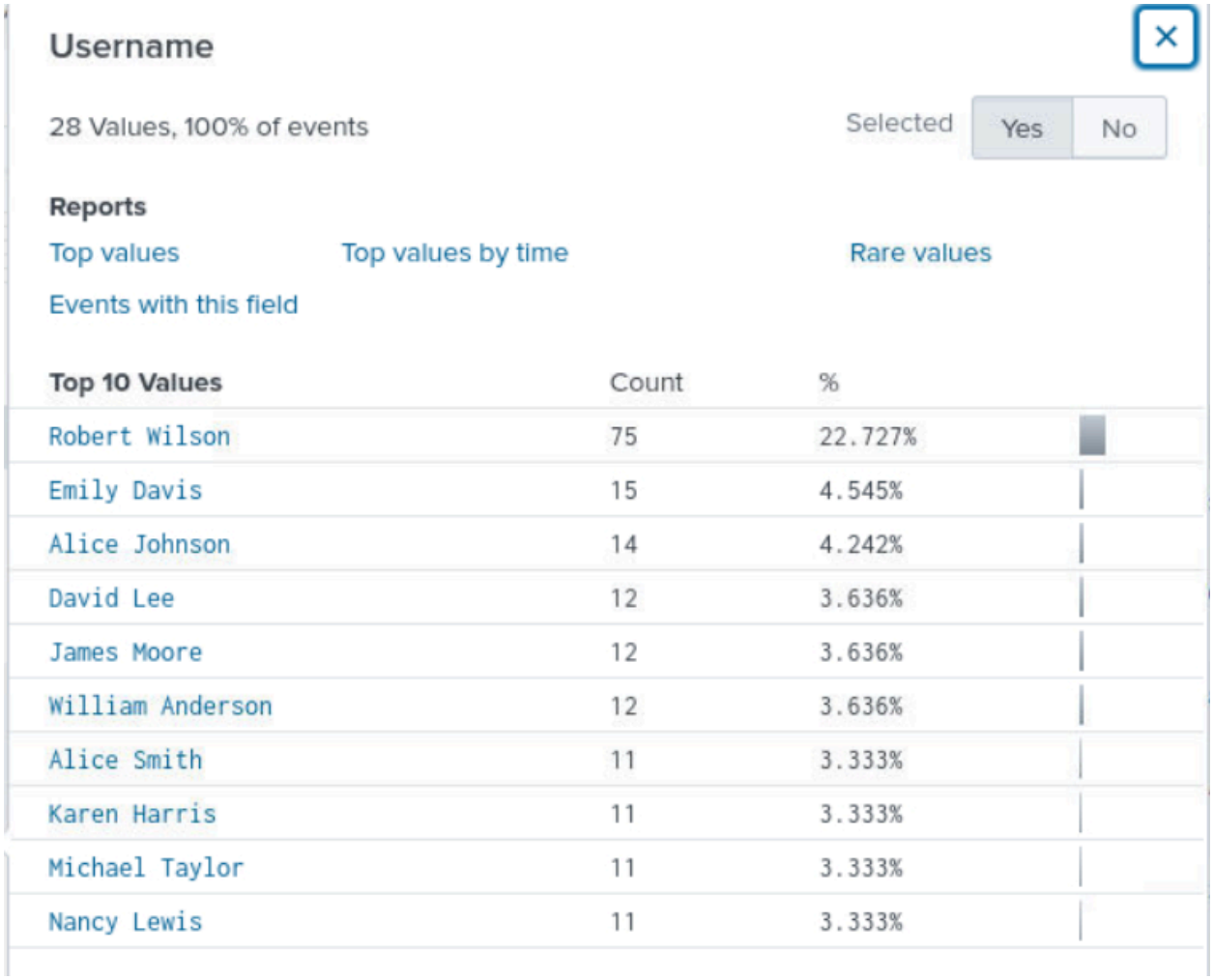
There are 12 different countries logged.
Answer: 12

How many departments are captured in the logs?



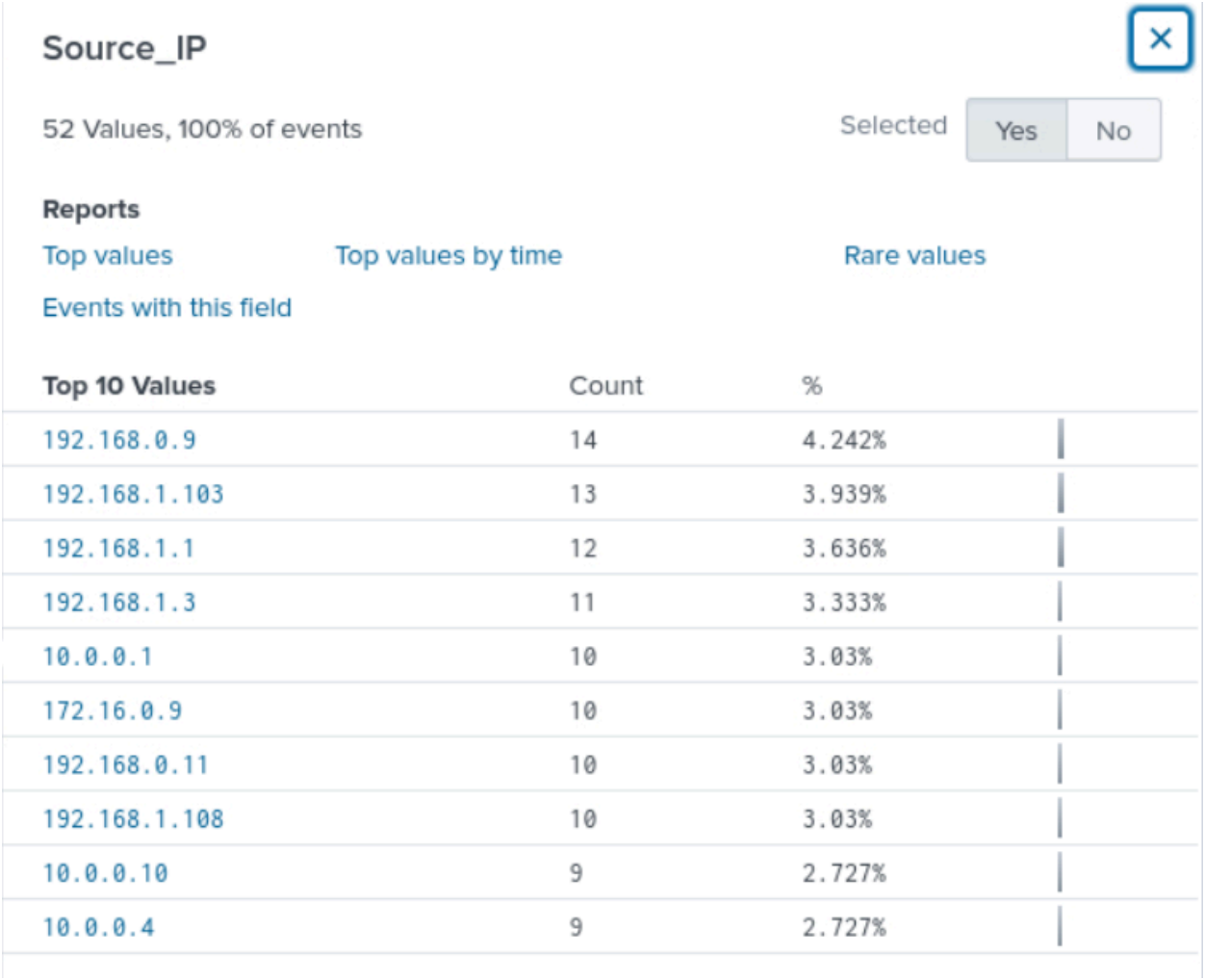
Answer: 6

How many usernames are captured in the logs?



Answer: 28

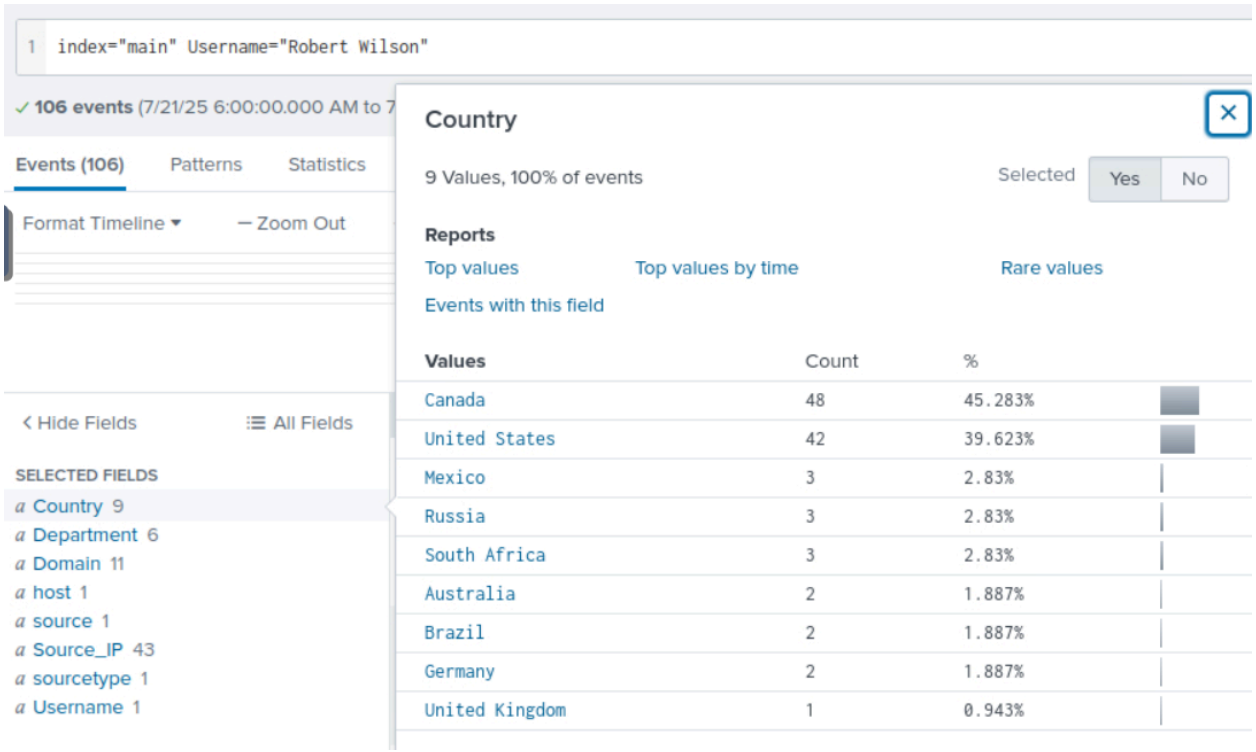
How many source IPs are captured in the logs?



Answer: 52

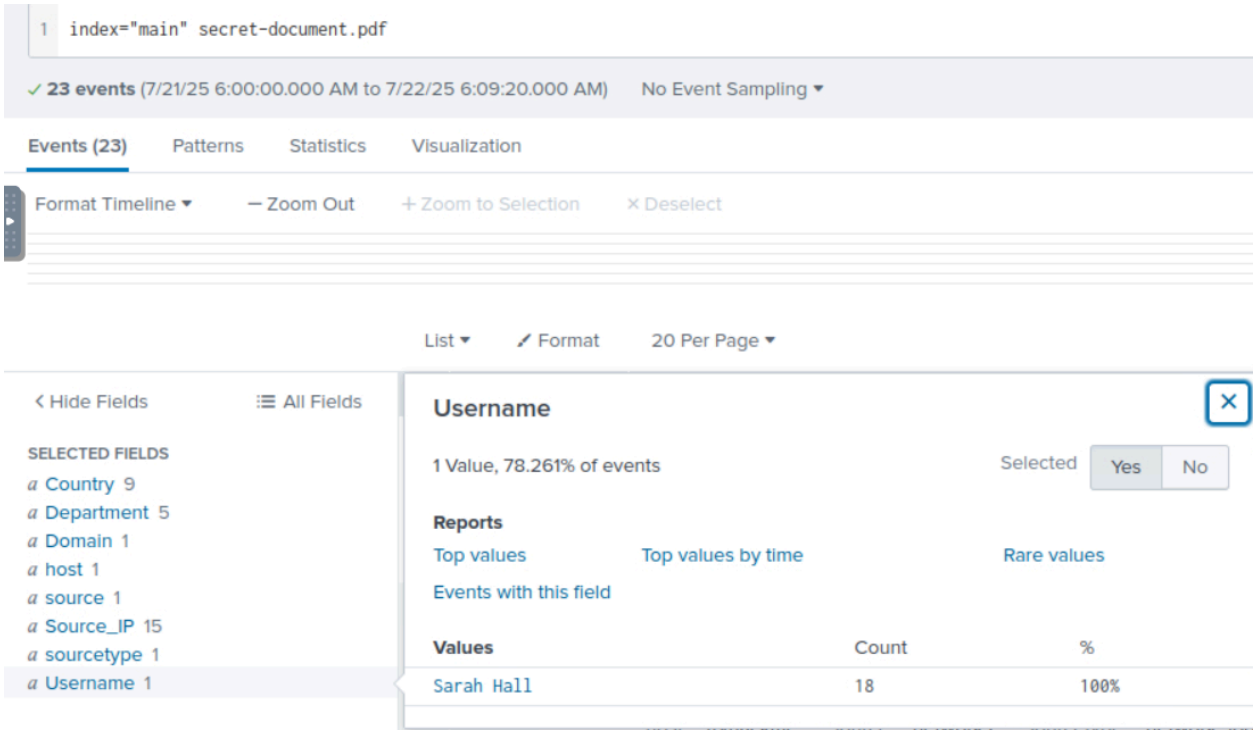
Which configuration files were used to fix our problem? [Alphabetic order: File1, file2, file3]
Answer: fields.conf, props.conf, transforms.conf

What are the TOP two countries the user Robert tried to access the domain from? [Answer in comma-separated and in Alphabetic Order][Format: Country1, Country2]



Filtering for just Robert Wilso we see the top two countries are Canada and the United States.
Answer: Canada, United States

Which user accessed the secret-document.pdf on the website?



Answer: Sarah Hall