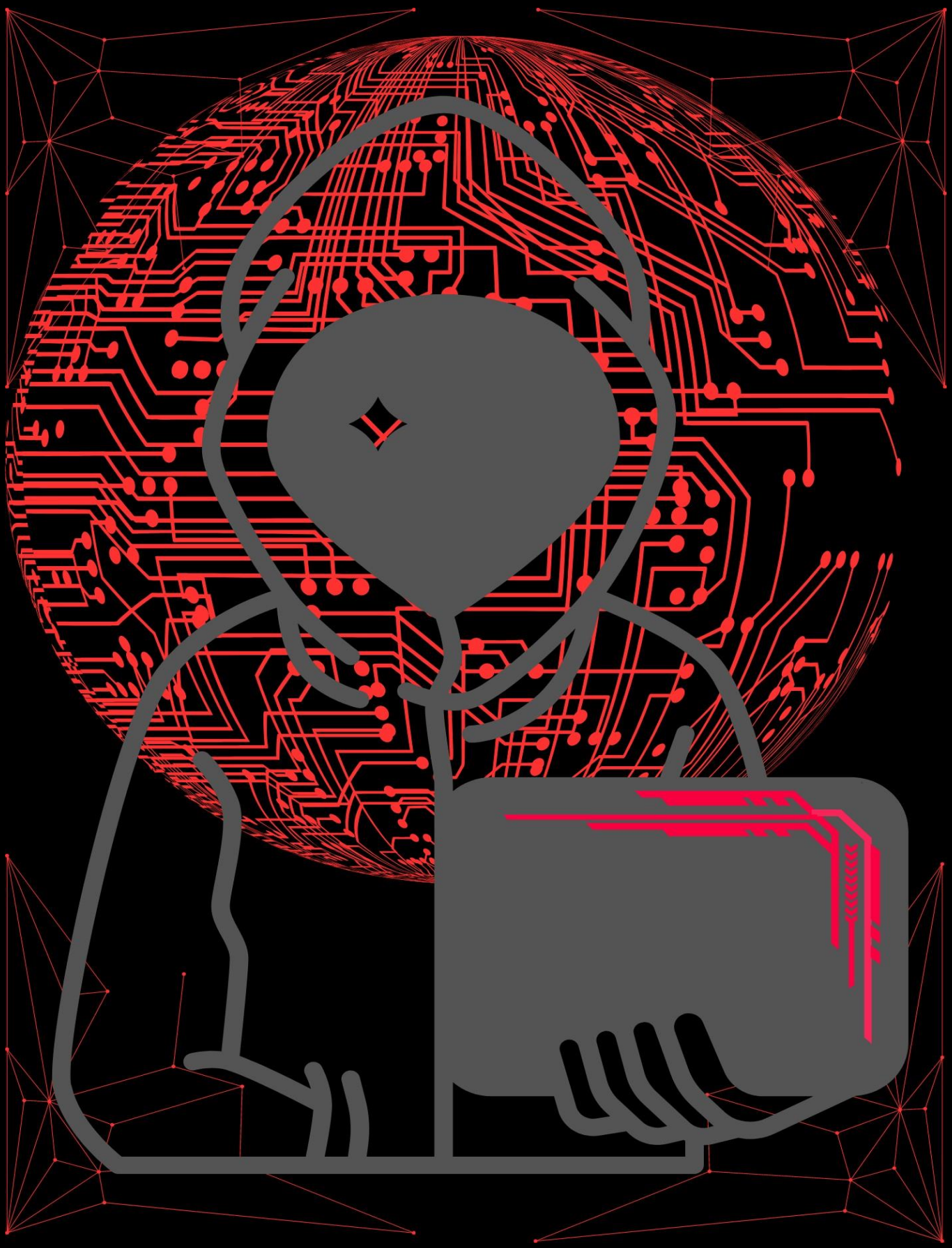
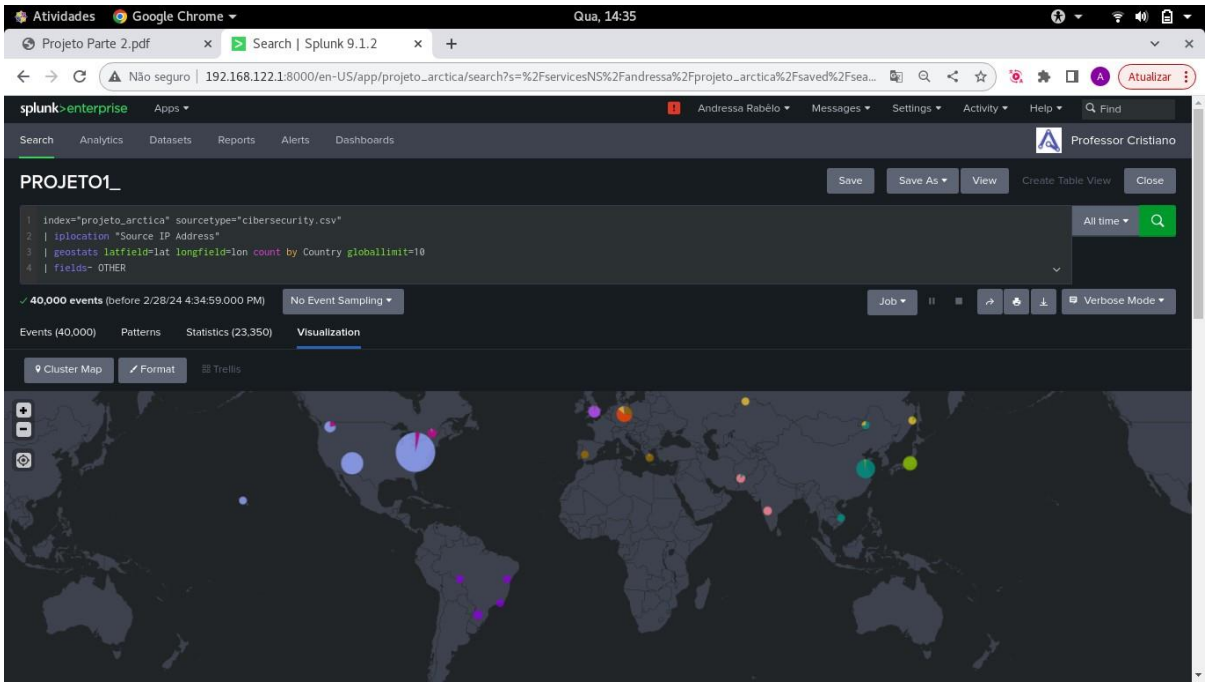


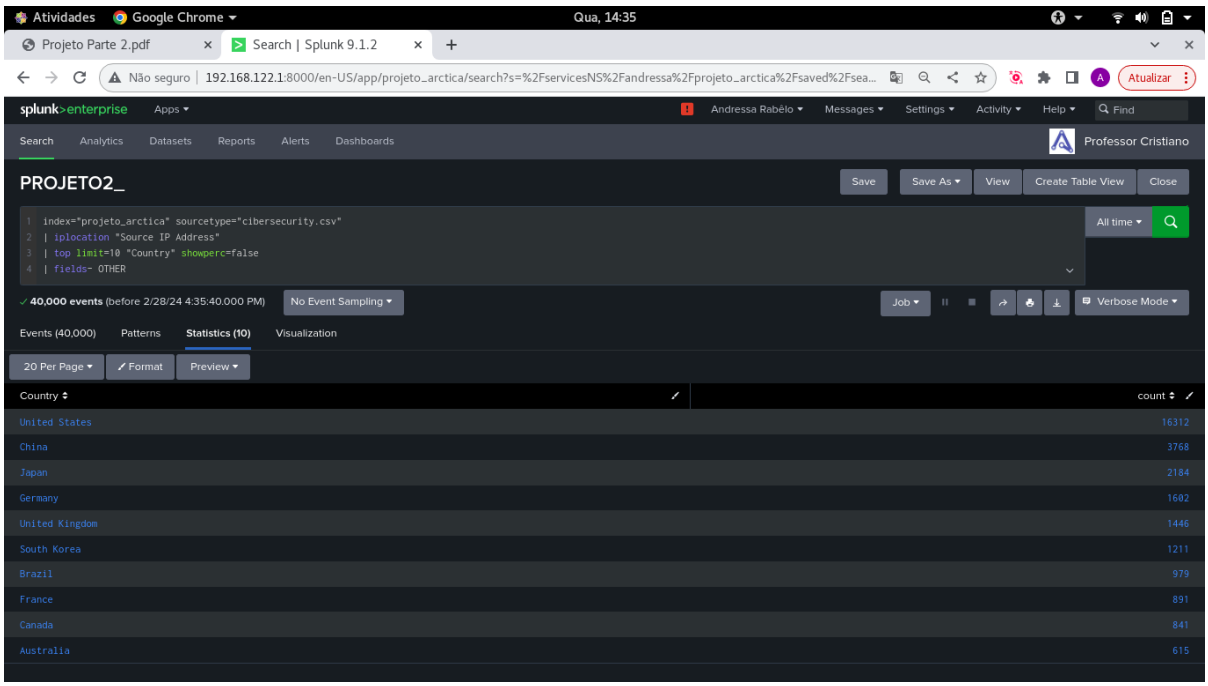
Andressa Emily Rabêlo Pereira
Dayane Francisca de Oliveira Vaz

PROJETO ARCTICA



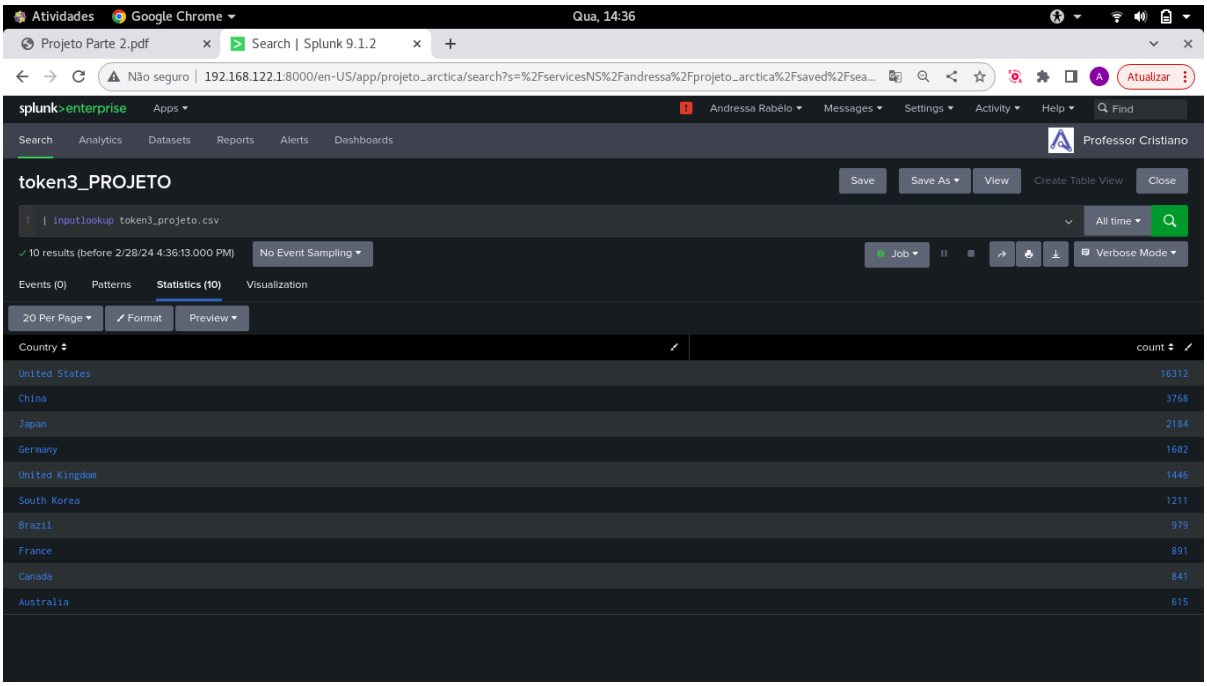
Atividade 1:

- | iplocation “Source IP Address”
  - Utilizamos esse comando para extrair informações de localização através do IP
  - Nome do campo onde os IPs de lançamento estavam armazenados;
- | geostats latfield=lat longfield=lon count by “Country” globallimit=10
  - Comando para gerar estatísticas geográficas (como latitude e longitude por exemplo) e gerar um resumo em mapa.
  - Foi utilizado para gerar um mapa com contagem por País;
  - Para limitar o número total dos resultados;
- | fields- OTHER
  - Utilizamos esse comando, junto ao operador aritmético (-) para retirar os falsos positivos da pesquisa;
  - Campo vazio.



Atividade 2:

- | iplocation “Source IP Address”
  - Utilizamos esse comando para extrair informações de localização através do IP
  - Nome do campo onde os IPs de lançamento estavam armazenados;
- | top limit=10 "Country" showperc=false
  - Foi utilizado o comando | top limit=10 para mostrar (como um ranking, por exemplo) os 10 países que mais lançaram ataques;
  - Para retirar as porcentagem (que aparecem quando utilizamos o comando | top;
- | fields- OTHER
  - Utilizamos esse comando, junto ao operador aritmético (-) para retirar os falsos positivos da pesquisa.
  - Campo vazio;



Atividade 3:

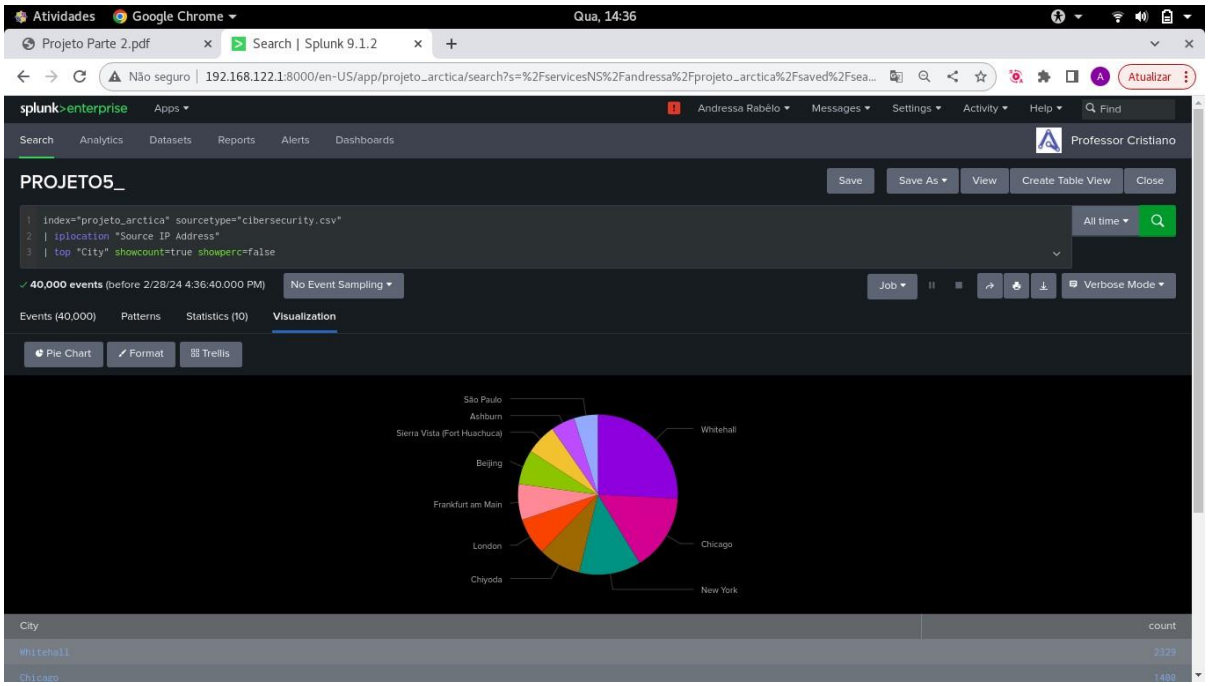
Criação da lookup (outputlookup):

- Foi utilizado a mesma pesquisa da 2 (segue abaixo), mas com a adição do comando | outputlookup

```
index="projeto_arctica"  sourcetype="cibersecurity.csv"
| iplocation "Source IP Address"
| top limit=10 "Country" showperc=false
| outputlookup token3_projeto.csv
```

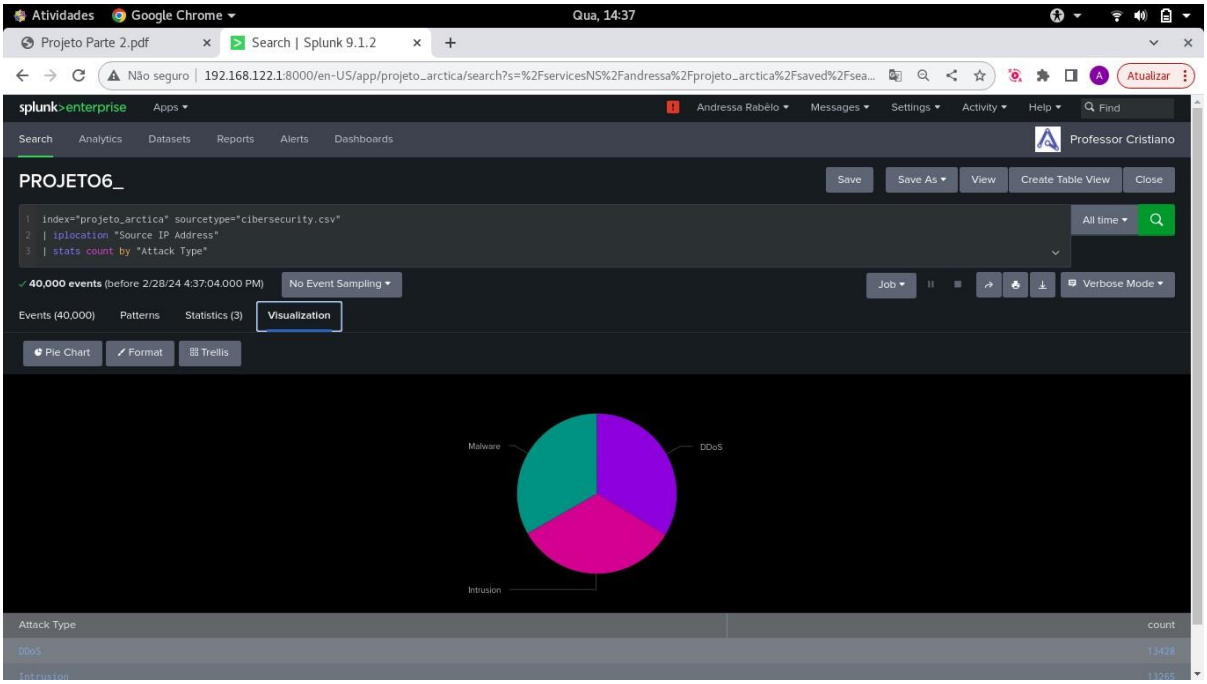
Chamar a lookup (inputlookup):

- | inputlookup token3_projeto.csv
    - Tal pesquisa, foi utilizada para difundir o token em todos os gráficos.



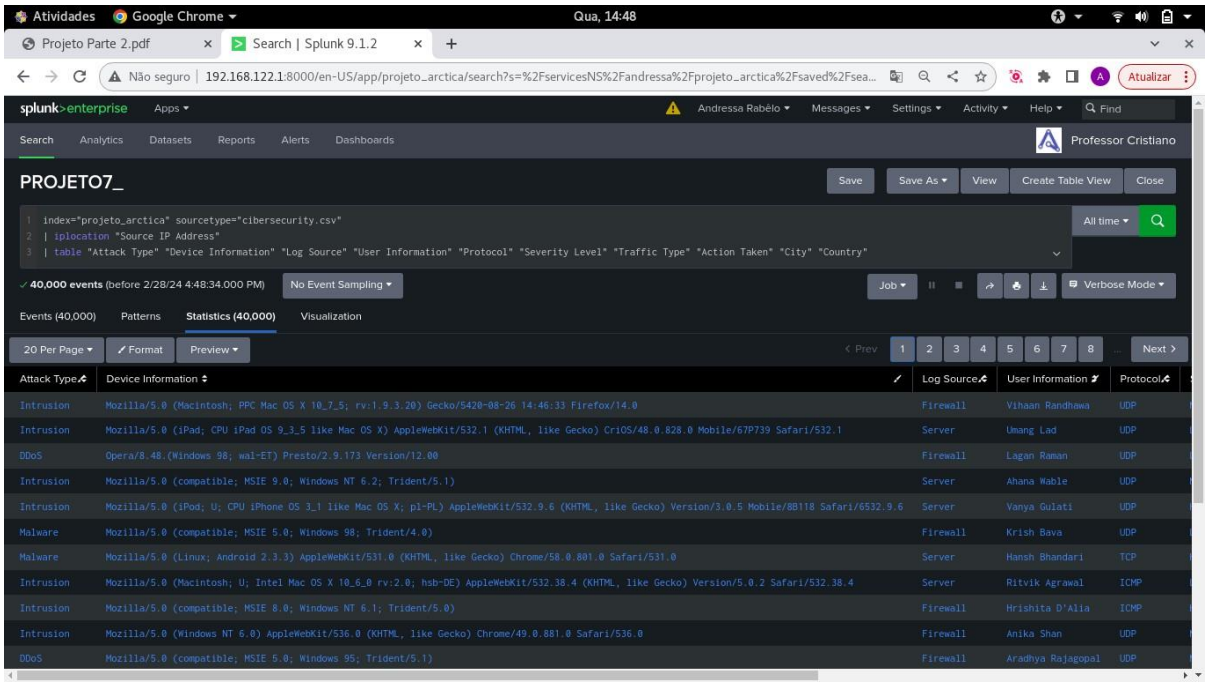
Atividade 5:

- | iplocation “Source IP Address”
    - Utilizamos esse comando para extrair informações de localização através do IP
    - Nome do campo onde os IPs de lançamento estavam armazenados;
- | top limit=10 "City" showcount= false showperc=false
    - Foi utilizado o comando | top limit=10 para mostrar (como um ranking, por exemplo) as 10 cidades que mais lançaram ataques;
    - Para retirar a contagem (que aparece quando utilizamos o comando | top;
    - Para retirar as porcentagem (que aparecem quando utilizamos o comando | top;



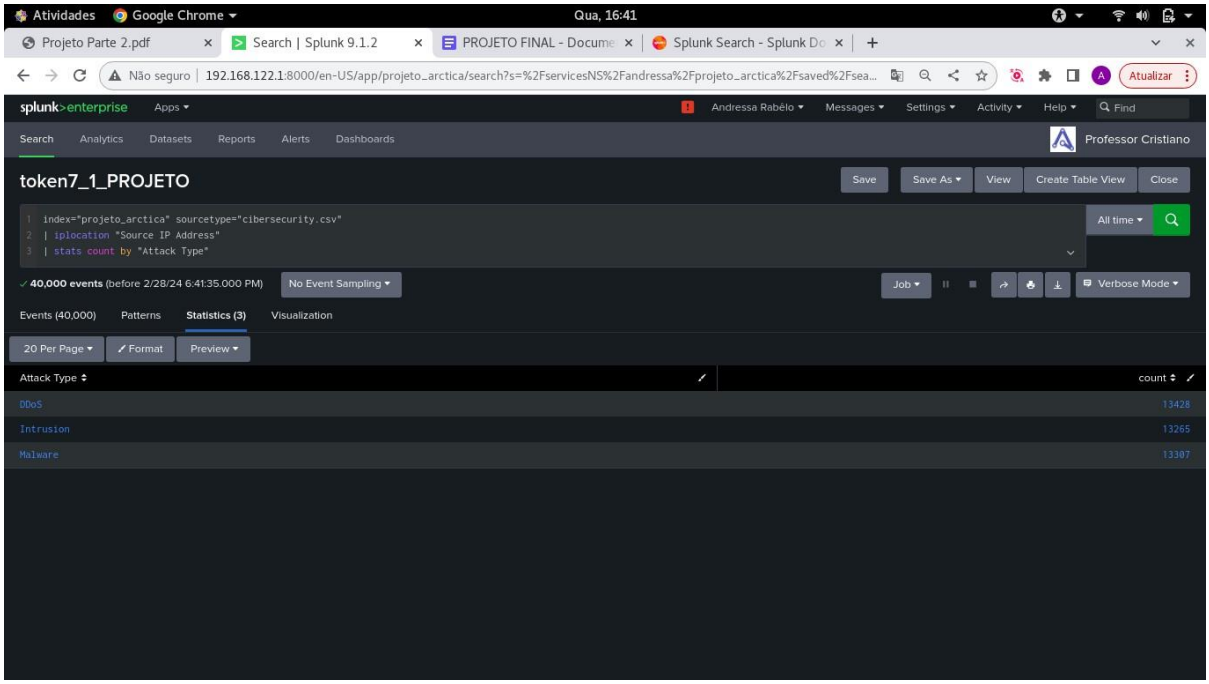
Atividade 6:

- | iplocation “Source IP Address”
    - Utilizamos esse comando para extrair informações de localização através do IP
    - Nome do campo onde os IPs de lançamento estavam armazenados;
- | stats count by "Attack Type"
    - Comando para mostrar a estatística de contagem por Tipo de ataque;



Atividade 7:

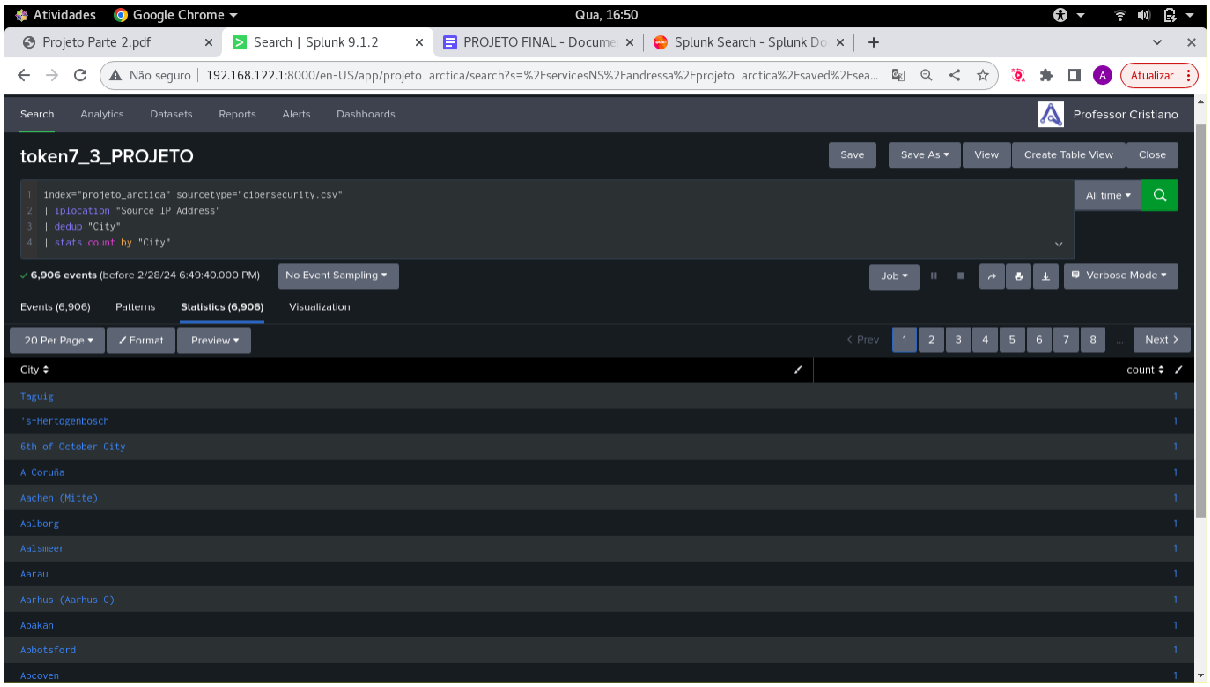
- | iplocation “Source IP Address”
    - Utilizamos esse comando para extrair informações de localização através do IP
    - Nome do campo onde os IPs de lançamento estavam armazenados;
- | table "Attack Type" "Device Information" "Log Source" "User Information" "Protocol" "Severity Level" "Traffic Type" "Action Taken" "City" "Country"
    - O comando | table foi usado para apenas criar uma tabela com os campos acima descritos;
    - Nome dos campos utilizados para a criação da tabela;



Token “Tipos de ataques” (ATIVIDADE 7):

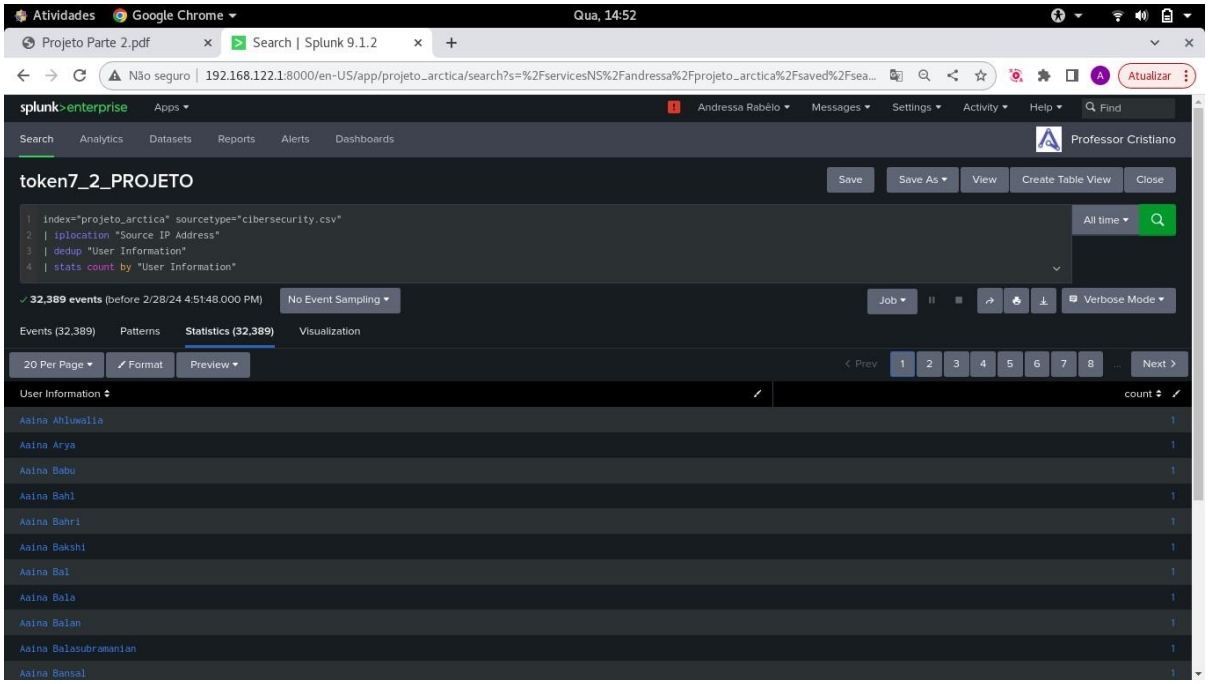
- | iplocation “Source IP Address”
    - Utilizamos esse comando para extrair informações de localização através do IP
    - Nome do campo onde os IPs de lançamento estavam armazenados;

- | stats count by "Attack Type"
    - Comando para mostrar a estatística de contagem por Tipo de ataque;



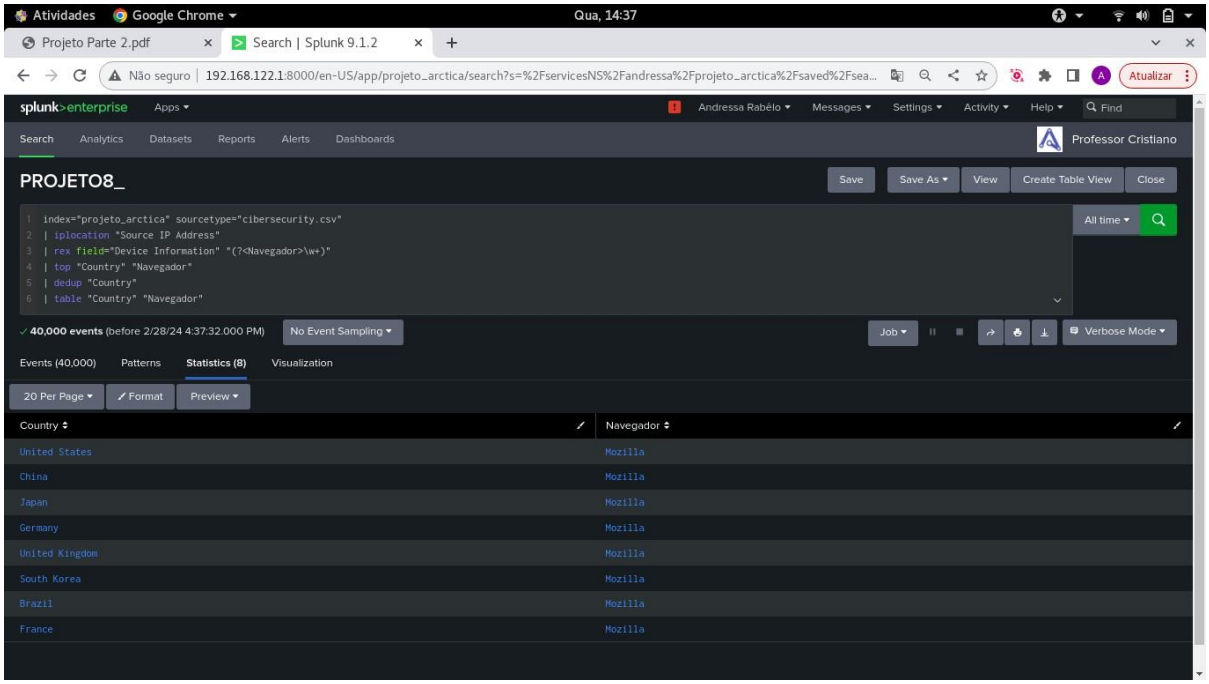
Token “Cidades” (ATIVIDADE 7):

- | iplocation “Source IP Address”
    - Utilizamos esse comando para extrair informações de localização através do IP
    - Nome do campo onde os IPs de lançamento estavam armazenados;
- | dedup "City"
- Comando usado para retirar os valores duplicados, nesse caso, o nome das Cidades;
- | stats count by "City"
    - Comando para mostrar a estatística de contagem por Cidades;



Token “Usuários” (ATIVIDADE 7):

- | iplocation “Source IP Address”
    - Utilizamos esse comando para extrair informações de localização através do IP
    - Nome do campo onde os IPs de lançamento estavam armazenados;
- | dedup "User Information"
- Comando usado para retirar os valores duplicados, nesse caso, o nome dos usuários;
- | stats count by "User Information"
    - Comando para mostrar a estatística de contagem por Usuário;

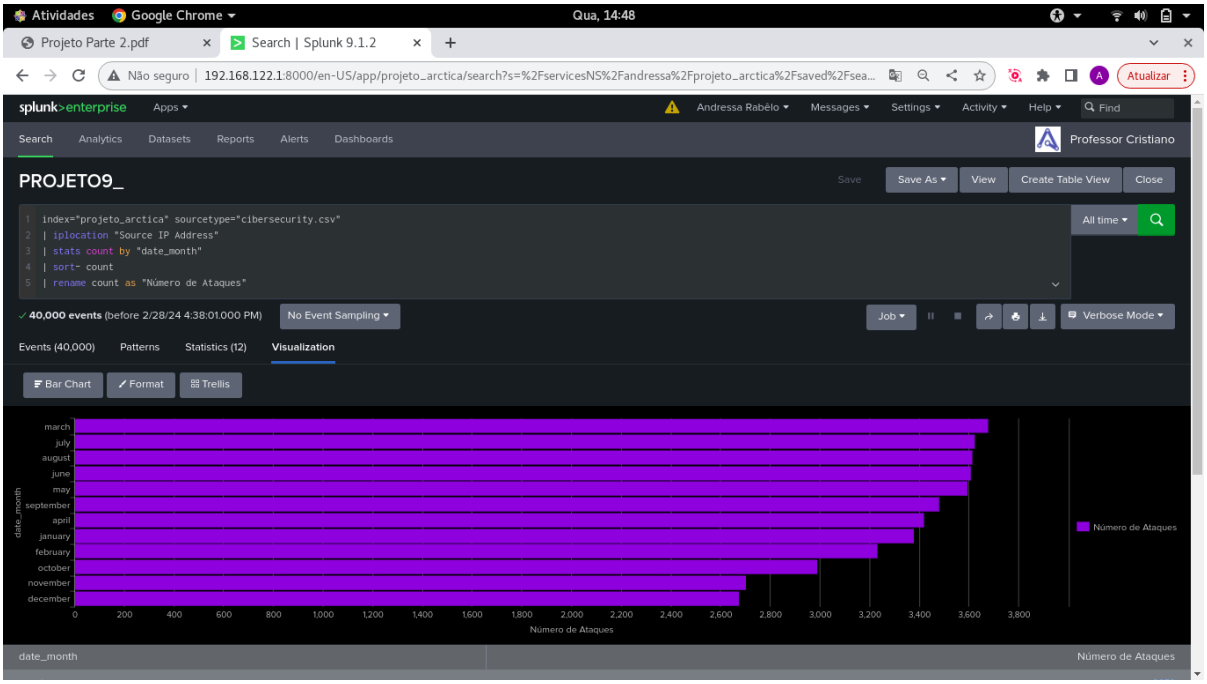


Atividade 8:

- | iplocation “Source IP Address”
    - Utilizamos esse comando para extrair informações de localização através do IP
    - Nome do campo onde os IPs de lançamento estavam armazenados;
- | rex field="Device Information" "(?<Navegador>\w+)"
    - O comando | rex field= é usado para extrair campos, nesse caso retirar apenas o nome do navegador;
    - Nome do campo de onde a informação será extraída;
    - Expressão para extrair apenas a primeira parte dos dados, parte essa onde está o navegador. Nesse processo foi criado o campo “Navegador”, onde ficam armazenados os navegadores.
- | top “Country” “Navegador”
    - Foi utilizado o comando | top para mostrar (como um ranking, por exemplo) os países que mais lançaram ataques e seus navegadores;

- | dedup "Country"
    - Comando usado para retirar os valores duplicados, nesse caso, o nome dos países;

- | table "Country" "Navegador"
    - O comando | table foi usado apenas para criar uma tabela com os campos acima descritos;
    - Nome dos campos utilizados para a criação da tabela;



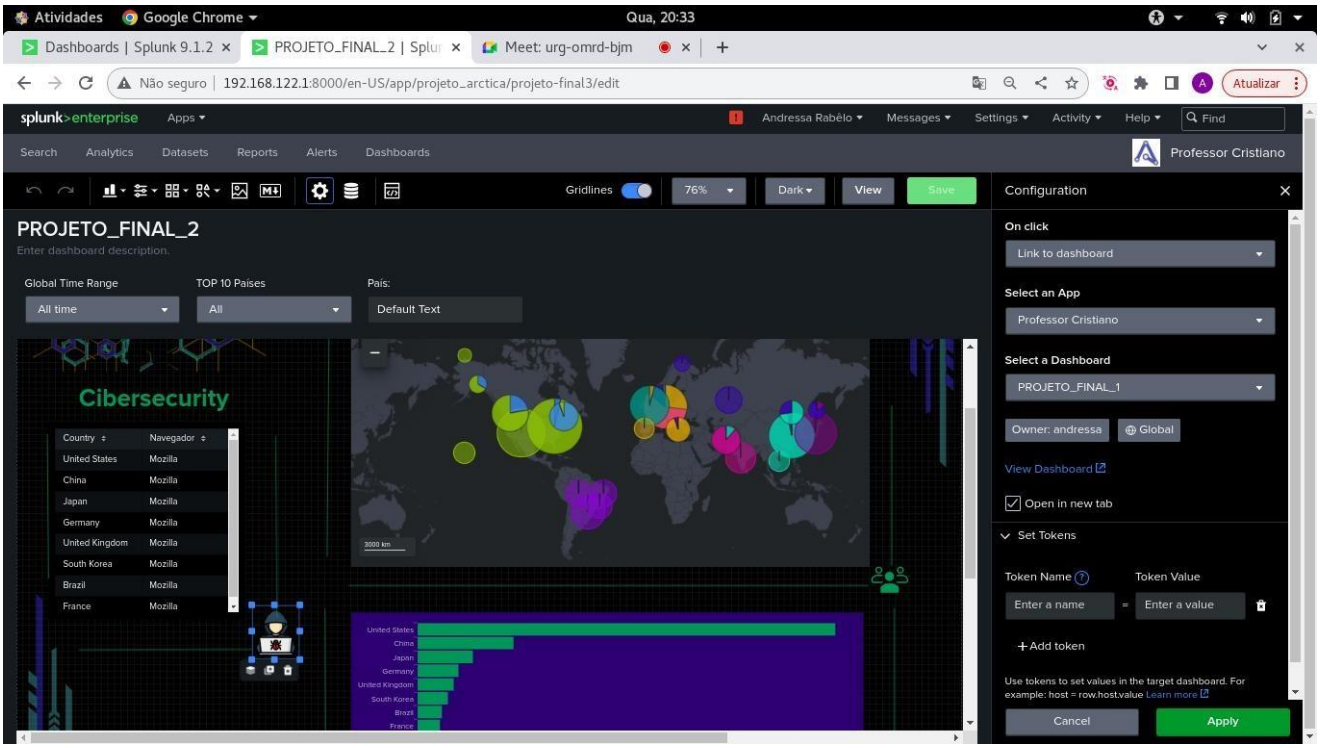
Atividade 9:

- | iplocation “Source IP Address”
    - Utilizamos esse comando para extrair informações de localização através do IP
    - Nome do campo onde os IPs de lançamento estavam armazenados;

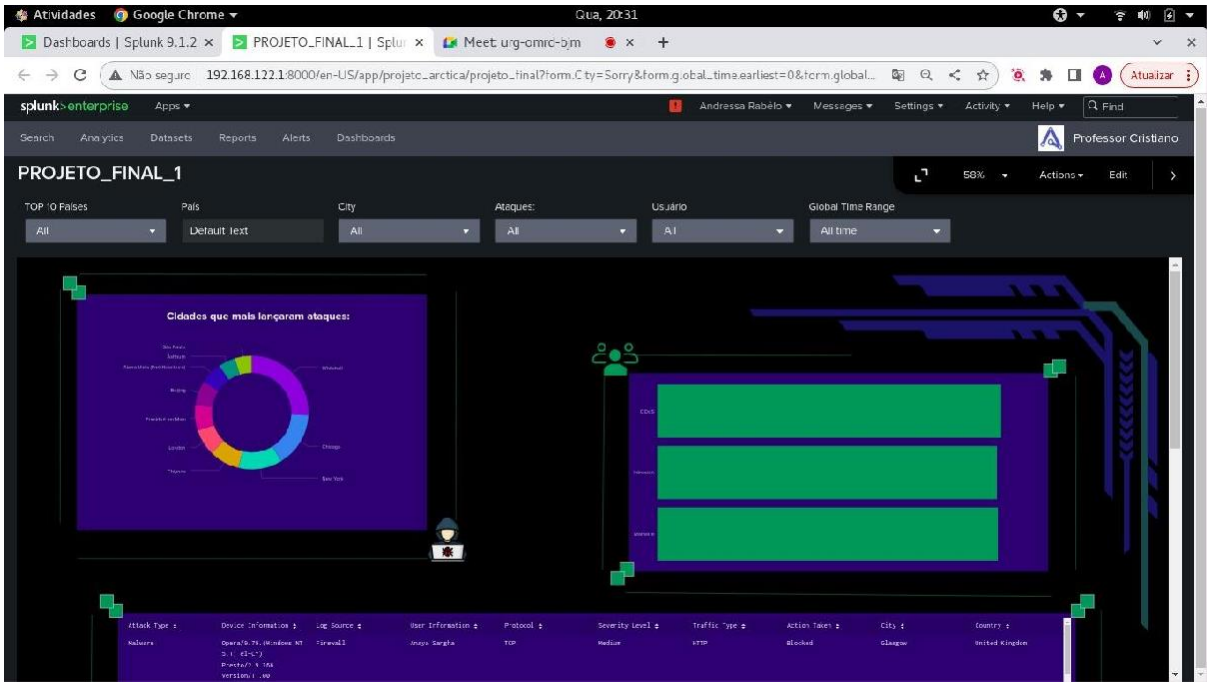
- | stats count by "date_month"
    - Comando para mostrar a estatística de contagem por Mês;

- | sort- count
    - O comando | sort é usando para ordenar, seguido do operador aritmético (-) ele ordena os países de acordo com a ordem decrescente das suas contagens;
    - Campo que será ordenado;

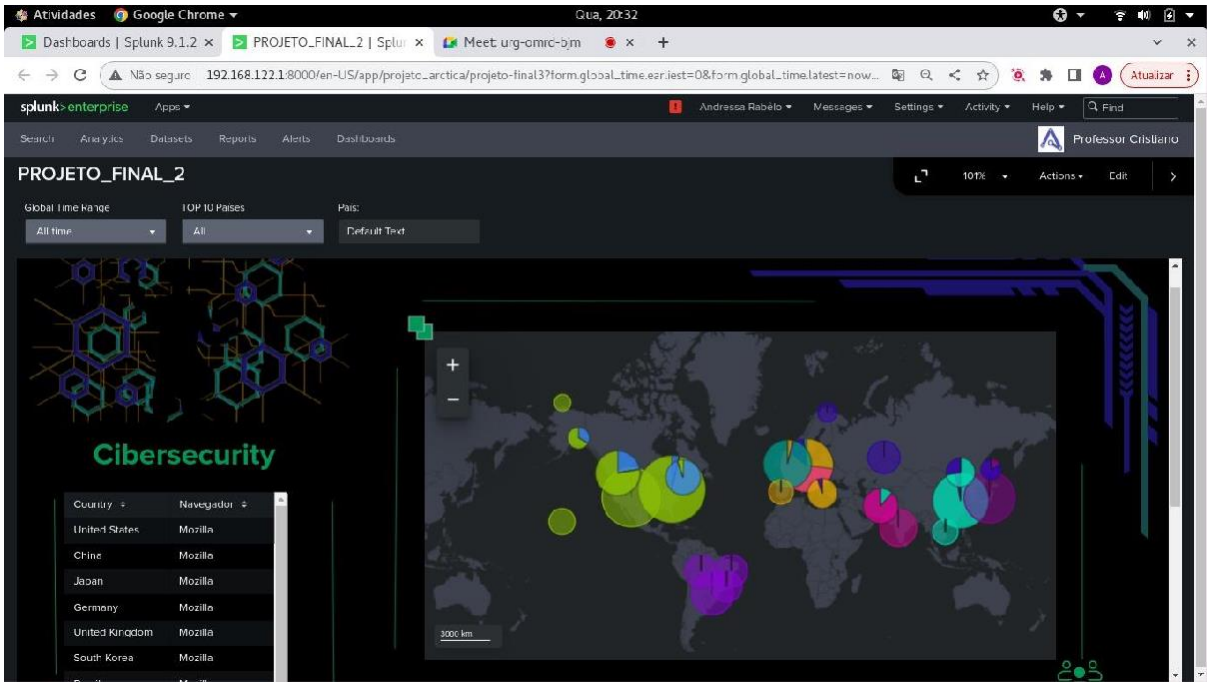
- | rename count as "Número de Ataques"
    - Esse comando foi usado para renomear um campo, no caso o “count”.
    - Campo renomeado;
    - Novo nome;



- Drilldown para ligar os dois dashboards;



- No primeiro dashboard temos os gráficos das atividades: 5, 6, 7 e 9;
- 3 filtros em dropdown filtrando apenas o gráfico 7 (City, Ataques, Usuário";
- 1 filtro em dropdown, filtrando todos os gráficos (TOP 10 Países);
- 1 filtro de texto para todos os gráficos (Países);
- 1 link via drildrown, conectando os 2 dashboards.



- No segundo dashboard temos os gráficos das atividades: 1, 2, e 8;
- 1 filtro em dropdown, filtrando todos os gráficos (TOP 10 Países);
- 1 filtro de texto para todos os gráficos (Países);
- 1 link via drildrown, conectando os 2 dashboards.

PROJETO_FINAL...

TOP 10 País... All | P... Default Text | City All | Ataqu... All | Usuár... All | Global Time Ran... All time

Cidades que mais lançaram ataques:

Attack	Device	Log	User	Protoc…	Severity	Traffic	Action	Ci…	Count…
Malware	Opera/9.79.(Windows NT 5.1; el-CY) Presto/2.9.166 Version/11.00	Firewall	Anaya Sangha	TCP	Medium	HTTP	Blocked	Glasgow	United Kingdom
Intrusion	Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/535.0 (KHTML, like Gecko) CriOS/15.0.821.0 Mobile/30N406 Safari/535.0	Server	Kiaan Samra	ICMP	Medium	DNS	Ignored	Chicago	United States
Malware	Mozilla/5.0 (iPod; U; CPU iPhone OS 4_2 like	Server	Nitara Mammen	TCP	High	FTP	Blocked	Tyler	United States

‹Prev 1 2 3 4 5 … Next›

CIBERSECURITY

PROJETO_FINAL...

Global Time Ran... All time

TOP 10 País... All

Pa... Default Text

Cibersecurity

Count...	Navegad...
United States	Mozilla
China	Mozilla
Japan	Mozilla
Germany	Mozilla
United Kingdom	Mozilla
South Korea	Mozilla
Brazil	Mozilla
France	Mozilla