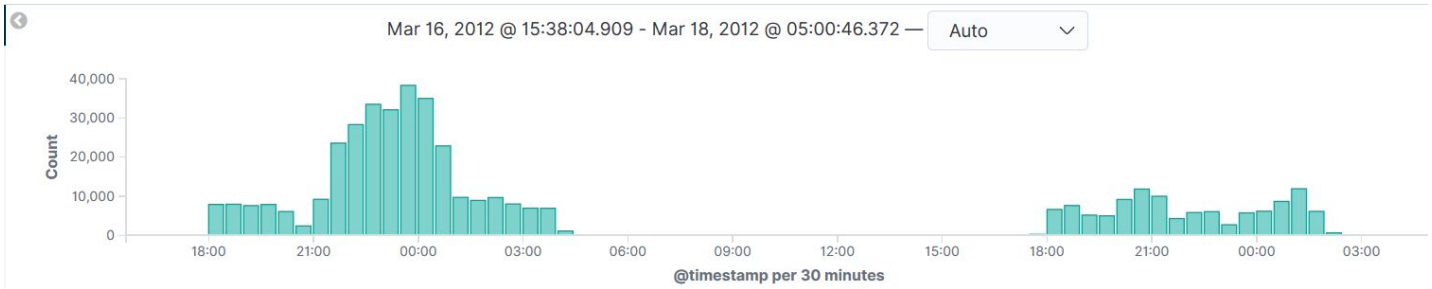
ATTACK DEFENSE

by PentesterAcademy

Name	Kibana : DNS Log Analysis
URL	https://attackdefense.com/challengedetails?cid=1191
Type	Log Analysis : DNS Logs

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Kibana Dashboard:



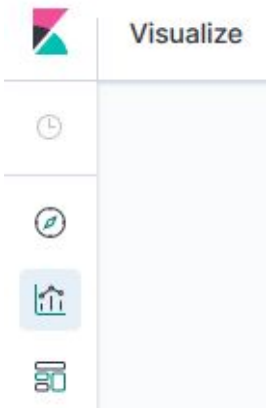
Time	sender_ip	sender_port	target_ip	target_port	query_type_desc	query	resp_code_desc
Mar 18, 2012 @ 02:29:51.970	192.168.202.122	137	192.168.202.255	137	NB	LABADMIN-641491	-
Mar 18, 2012 @ 02:29:39.080	192.168.202.83	45561	192.168.207.4	53	PTR	44.206.168.192.in-addr.arpa	NXDOMAIN
Mar 18, 2012 @ 02:29:19.830	192.168.202.88	65208	192.168.206.44	53	PTR	lb._dns-sd._udp.0.48.16.172.in-addr.arpa	REFUSED
Mar 18, 2012 @ 02:29:19.830	192.168.202.88	58045	192.168.206.44	53	PTR	b._dns-sd._udp.0.48.16.172.in-addr.arpa	REFUSED
Mar 18, 2012 @ 02:29:19.830	192.168.202.88	58547	192.168.206.44	53	PTR	dr._dns-sd._udp.0.202.168.192.in-addr.arpa	REFUSED

Q1. Provide the name of the most queried domain.

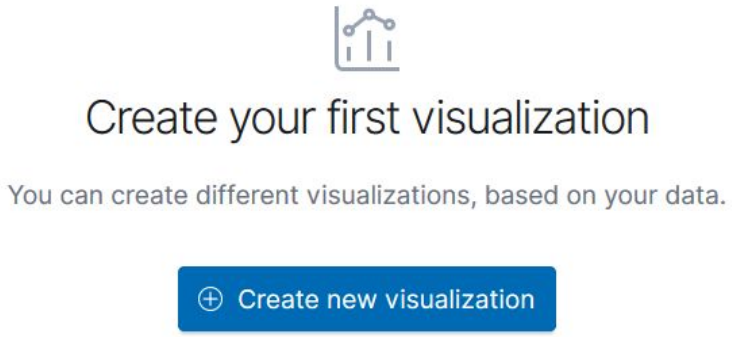
Ans: teredo.ipv6.microsoft.com

Solution:

Step 1: Create a visualization to figure this out. Navigate to the 'Visualize' Section.



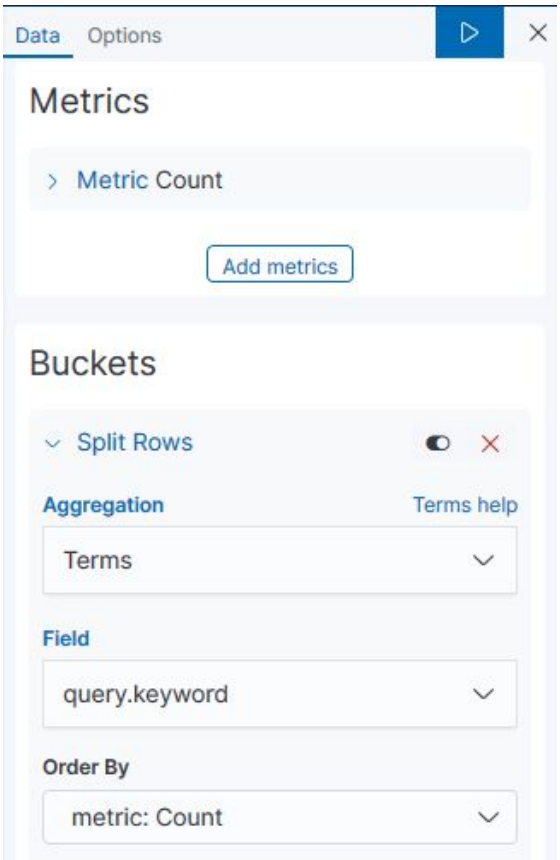
Step 2: Click on 'Create new visualization'.



Step 3: Select 'Data Table' Visualization.

Step 4: Choose the logstash-* index pattern as the source.

Step 5: Split the rows by applying 'Terms' aggregation on 'query.keyword' field.



Step 6: Press the 'Apply changes' button.

query.keyword: Descending	Count
teredo.ipv6.microsoft.com	39,273
tools.google.com	14,057
www.apple.com	13,390
time.apple.com	13,109
safebrowsing.clients.google.com	11,658

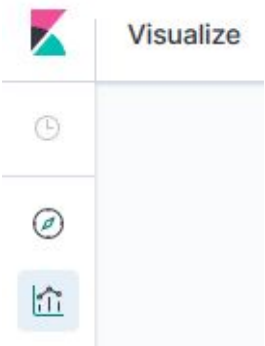
The most queried domain name was "teredo.ipv6.microsoft.com".

Q2. What was the IP address of the machine which issued a maximum number of requests having empty DNS queries?

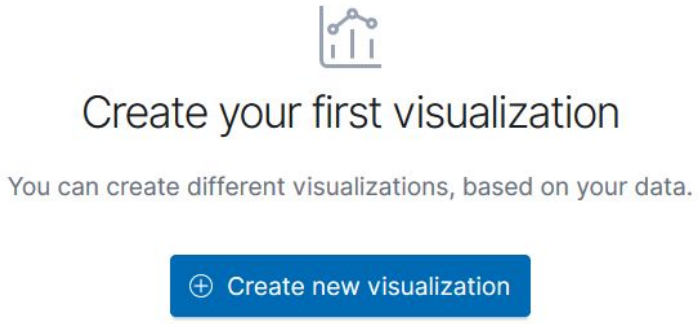
Ans: 192.168.202.78

Solution:

Step 1: Create a visualization to figure this out. Navigate to the 'Visualize' Section.



Step 2: Click on 'Create new visualization'.



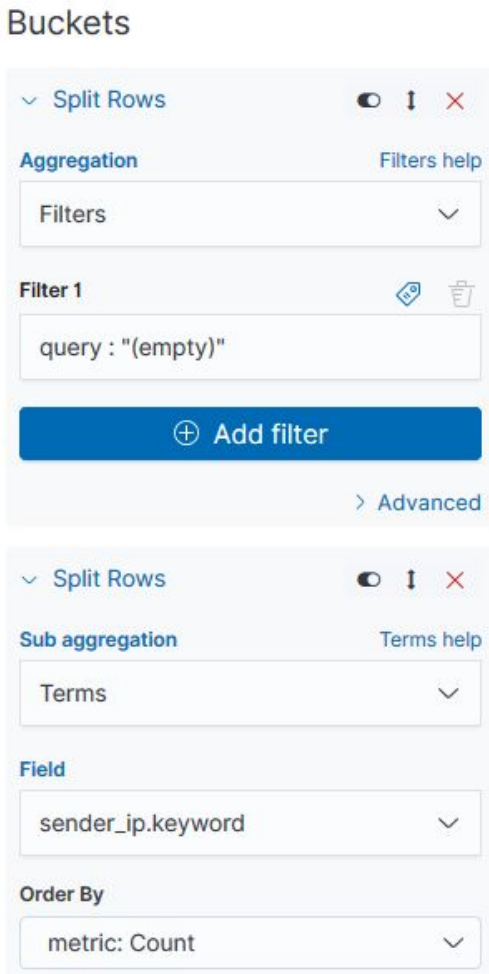
Step 3: Select 'Data Table' Visualization.

Step 4: Choose the logstash-* index pattern as the source.

Step 5: Split the rows by applying the following 'Filters' Aggregation:

FIlter: query : "(empty)"

And, apply a 'Terms' sub-aggregation on the field 'sender_ip.keyword' to get the IP address of the machine that sent the maximum number of empty DNS queries.



filters	sender_ip.keyword: Descending	Count
query : "(empty)"	192.168.202.78	860
query : "(empty)"	192.168.202.137	523
query : "(empty)"	192.168.202.71	421
query : "(empty)"	192.168.202.77	335
query : "(empty)"	192.168.202.139	185

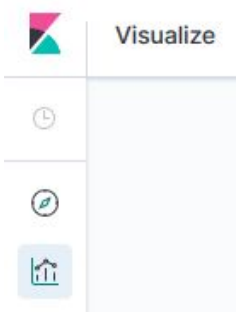
The host with IP address 192.168.202.78 issued the maximum number of empty DNS queries.

Q3. What was the IP address of the machine that received a maximum number of NXDOMAIN responses?

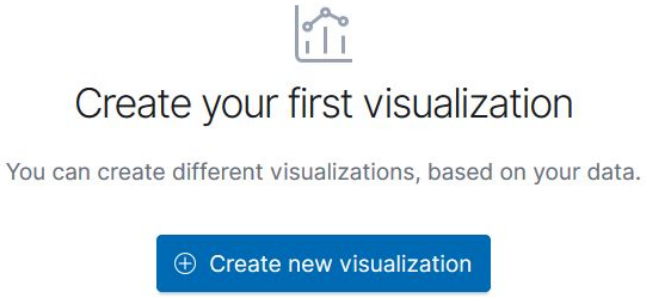
Ans: 192.168.202.103

Solution:

Step 1: Create a visualization to figure this out. Navigate to the 'Visualize' Section.



Step 2: Click on 'Create new visualization'.



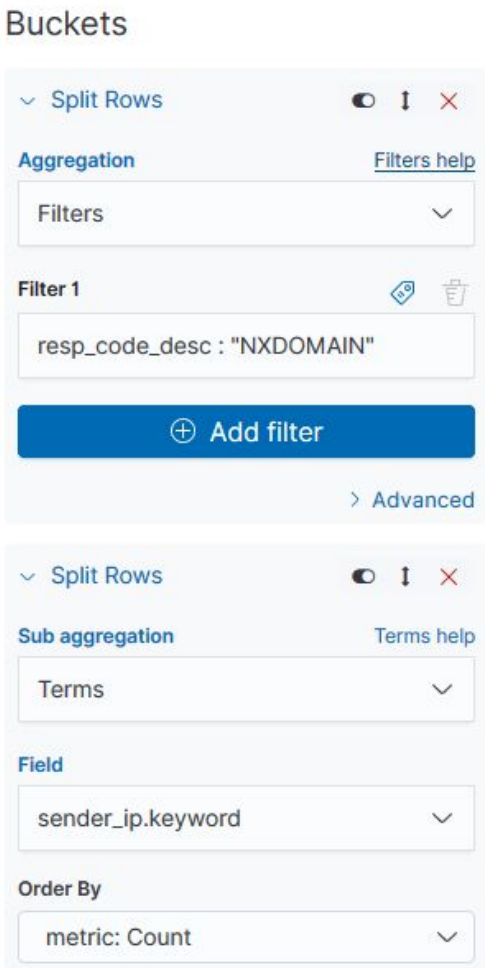
Step 3: Select 'Data Table' Visualization.

Step 4: Choose the logstash-* index pattern as the source.

Step 5: Split the rows by applying the following 'Filters' Aggregation:

Filter: resp_code_desc : "NXDOMAIN"

And, apply a 'Terms' sub-aggregation on the field 'sender_ip.keyword' to get the IP address of the machine that received the most NXDOMAIN errors.



filters	sender_ip.keyword: Descending	Count
resp_code_desc : "NXDOMAIN"	192.168.202.103	7,471
resp_code_desc : "NXDOMAIN"	192.168.202.138	4,762
resp_code_desc : "NXDOMAIN"	192.168.202.79	4,711
resp_code_desc : "NXDOMAIN"	192.168.202.83	4,453
resp_code_desc : "NXDOMAIN"	192.168.202.140	3,835

The host with IP address 192.168.202.103 received the most NXDOMAIN responses.

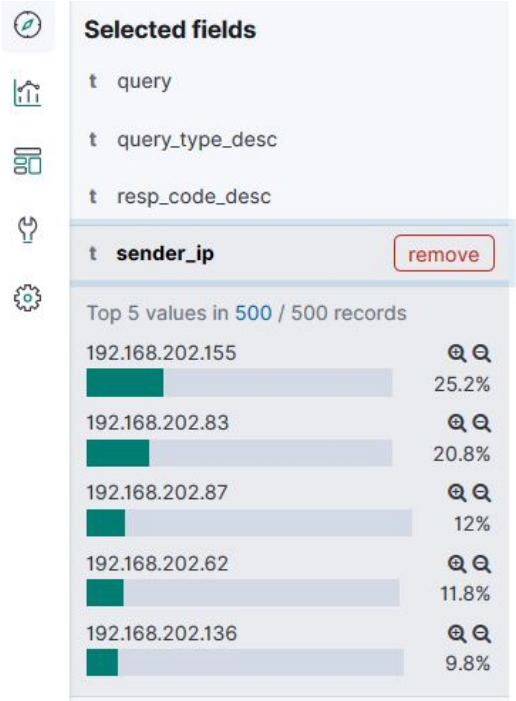
Q4. For one of the hosts receiving NXDOMAIN errors, could you figure out some anomalous behavior? If yes, then describe the behavior.

Solution:

Step 1: Apply the following filter to view all the DNS logs in which the response is NXDOMAIN.

Filter: resp_code_desc : "NXDOMAIN"

Step 2: Check the top 5 sender IP addresses from the Selected Fields on the left panel.

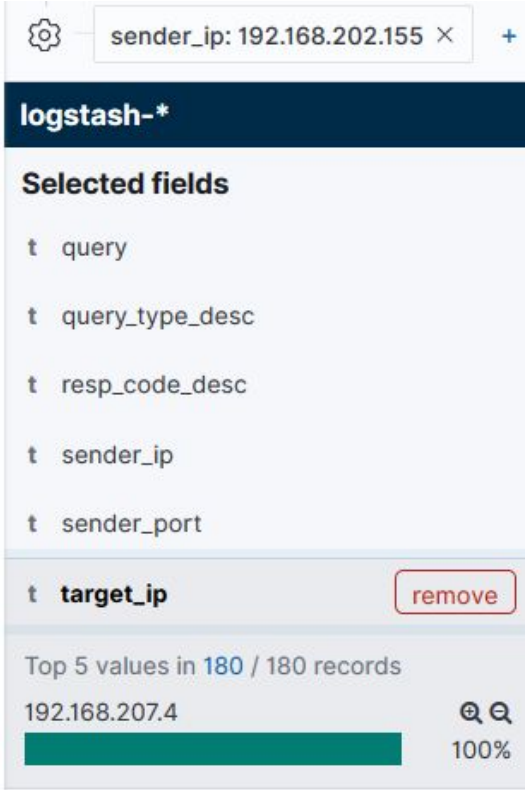


Step 3: Click on the zoom-in icon for the first sender IP address in the list and examine the queries that were issued by that host.

Time	sender_ip	sender_port	target_ip	target_port	query_type_desc	query	resp_code_desc
Mar 18, 2012 @ 02:05:40.020	192.168.202.155	52746	192.168.207.4	53	A	jigsaw.w3.org	NXDOMAIN
Mar 18, 2012 @ 02:05:40.020	192.168.202.155	37546	192.168.207.4	53	A	dokuwiki.org	NXDOMAIN
Mar 18, 2012 @ 02:05:40.020	192.168.202.155	48981	192.168.207.4	53	A	validator.w3.org	NXDOMAIN
Mar 18, 2012 @ 02:05:40.010	192.168.202.155	49846	192.168.207.4	53	AAAA	dokuwiki.org	NXDOMAIN
Mar 18, 2012 @ 02:05:40.010	192.168.202.155	37090	192.168.207.4	53	AAAA	validator.w3.org	NXDOMAIN
Mar 18, 2012 @ 02:05:40.010	192.168.202.155	39330	192.168.207.4	53	A	www.php.net	NXDOMAIN
Mar 18, 2012 @ 02:05:40.010	192.168.202.155	49915	192.168.207.4	53	A	dokuwiki.org	NXDOMAIN
Mar 18, 2012 @ 02:05:40.010	192.168.202.155	41156	192.168.207.4	53	A	www.dokuwiki.org	NXDOMAIN

Observe that all the domains for which the queries were sent are legitimate and should be accessible. But the requests result in NXDOMAIN error. There was some issue with the DNS server in this scenario.

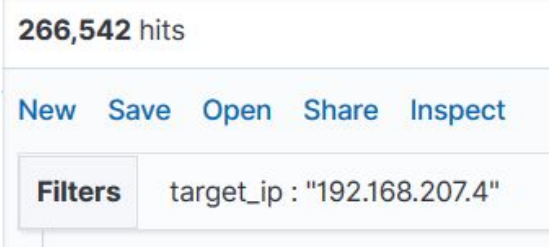
Step 4: Check the target_ip field from the Selected Fields in the left pane.



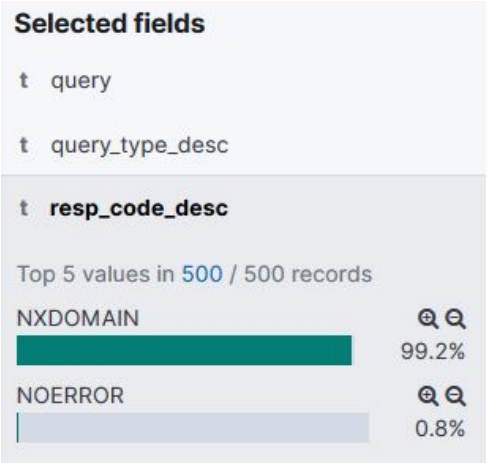
There was some issue with that DNS server running on IP address 192.168.207.4.

Step 5: To confirm this, apply the following filter to get all the logs where the target IP address was 192.168.207.4.

Filter: target_ip : "192.168.207.4"



Step 6: Check the resp_code_desc field from the Selected Fields in the left pane.



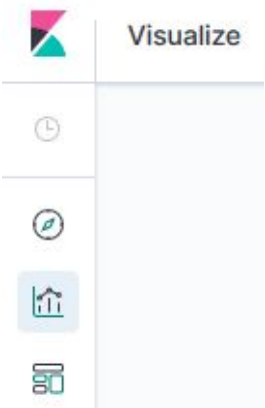
The DNS server at 192.168.207.4 generated NXDOMAIN error 99.2% of the time.

Q5. What was the IP address of the machine that sent the most DNS requests?

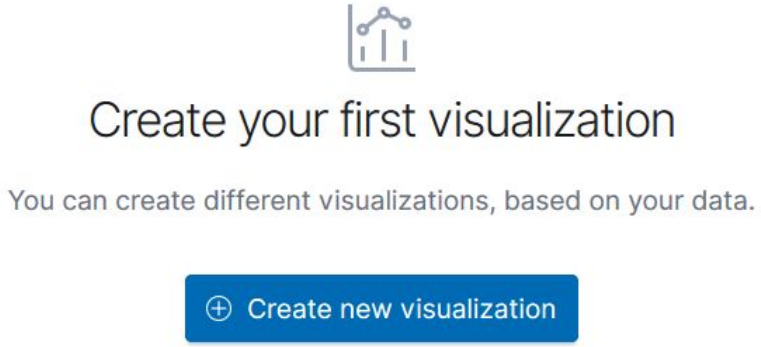
Ans: 10.10.117.210

Solution:

Step 1: Create a visualization to figure this out. Navigate to the 'Visualize' Section.



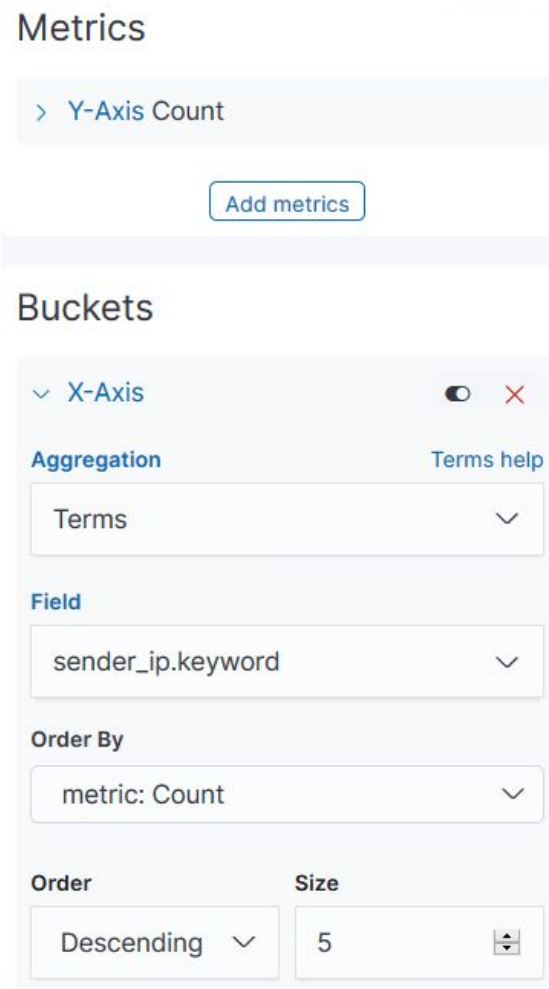
Step 2: Click on 'Create new visualization'.



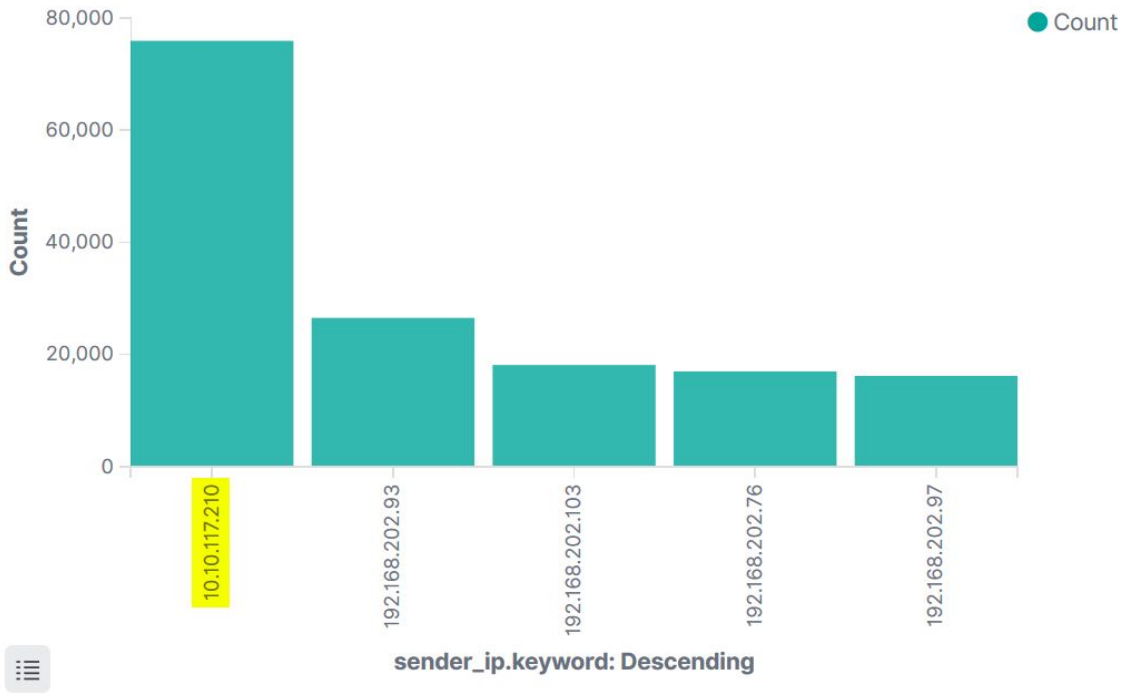
Step 3: Select 'Vertical Bar' Visualization.

Step 4: Choose the logstash-* index pattern as the source.

Step 5: Split the X-Axis by applying 'Terms' aggregation on 'sender_ip.keyword' field.



Step 6: Press the 'Apply changes' button.



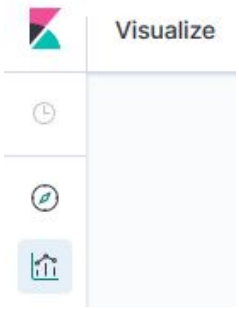
The host with the IP address "10.10.117.210" sent the most DNS requests.

Q6. What was the IP address of the machine that sent the most reverse DNS resolution requests?

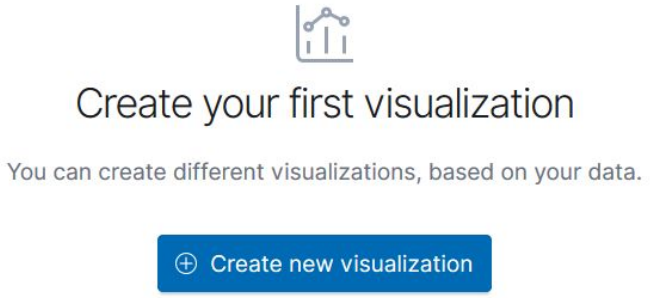
Ans: 192.168.202.83

Solution:

Step 1: Create a visualization to figure this out. Navigate to the 'Visualize' Section.



Step 2: Click on 'Create new visualization'.



Step 3: Select 'Data Table' Visualization.

Step 4: Choose the logstash-* index pattern as the source.

Step 5: Split the rows by applying the following 'Filters' Aggregation:

Filter: query : "*in-addr.arpa"

And, apply a 'Terms' sub-aggregation on the field 'sender_ip.keyword' to get the IP address of the machine that sent the most reverse DNS resolution queries.

Buckets

Split Rows

Aggregation — Filters help

Filters

Filter 1

query : "*in-addr.arpa"

Add filter

Advanced

Split Rows

Sub aggregation — Terms help

Terms

Field

sender_ip.keyword

Order By

metric: Count

filters	sender_ip.keyword: Descending	Count
query : "*in-addr.arpa"	192.168.202.83	7,283
query : "*in-addr.arpa"	192.168.202.110	6,118
query : "*in-addr.arpa"	192.168.202.97	5,837
query : "*in-addr.arpa"	192.168.202.106	3,612
query : "*in-addr.arpa"	192.168.202.79	3,566
query : "*in-addr.arpa"	192.168.202.138	3,430
query : "*in-addr.arpa"	192.168.202.84	2,511
query : "*in-addr.arpa"	192.168.202.140	2,496
query : "*in-addr.arpa"	192.168.229.252	1,815
query : "*in-addr.arpa"	192.168.202.71	1,603

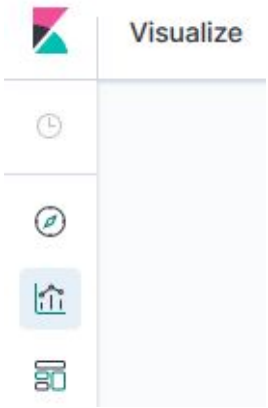
The host with IP address 192.168.202.83 sent the most reverse DNS resolution requests.

Q7. How many DNS zone transfer queries were issued on the network?

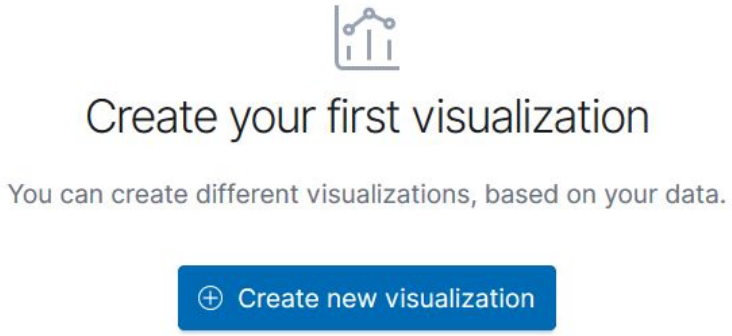
Ans: 440

Solution:

Step 1: Create a visualization to figure this out. Navigate to the 'Visualize' Section.



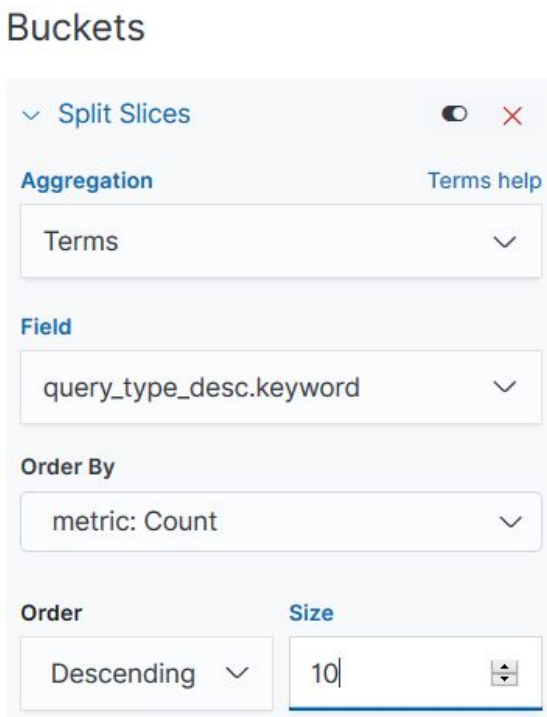
Step 2: Click on 'Create new visualization'.



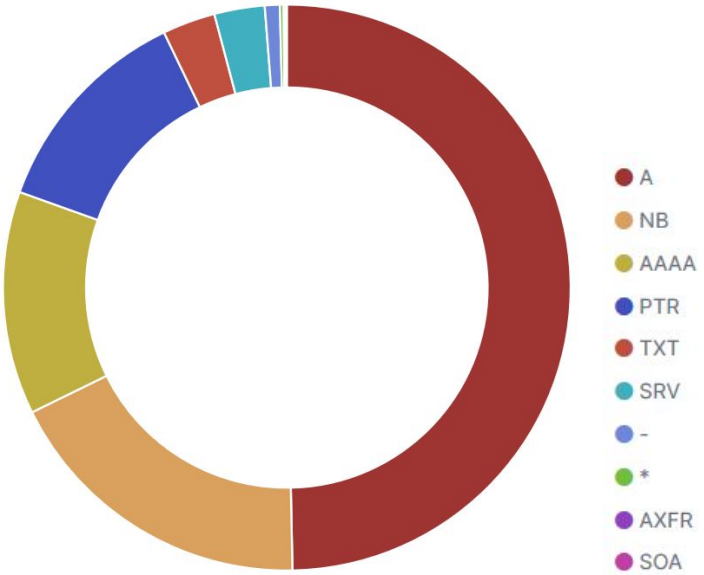
Step 3: Select 'Pie' Visualization.

Step 4: Choose the logstash-* index pattern as the source.

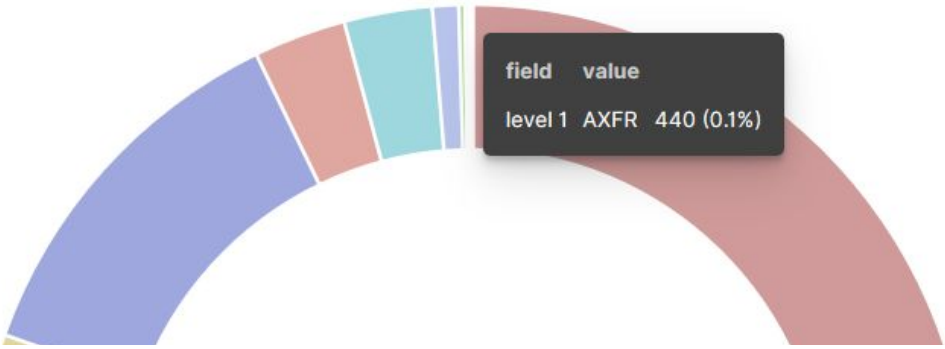
Step 5: Split the slices by applying 'Terms' aggregation on 'query_type_desc.keyword' field.



Step 6: Press the 'Apply changes' button.



Select the AXFR records and view their count.



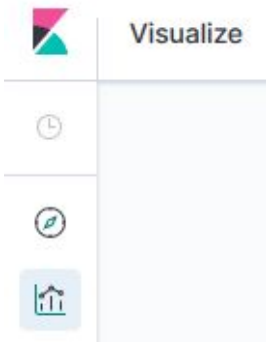
There were 440 DNS Zone Transfer (AXFR) records.

Q8. One of the DNS requests querying for a sub-domain of apple.com returned a TXT record which contained a suspicious looking answer. Identify the connection ID of that request.

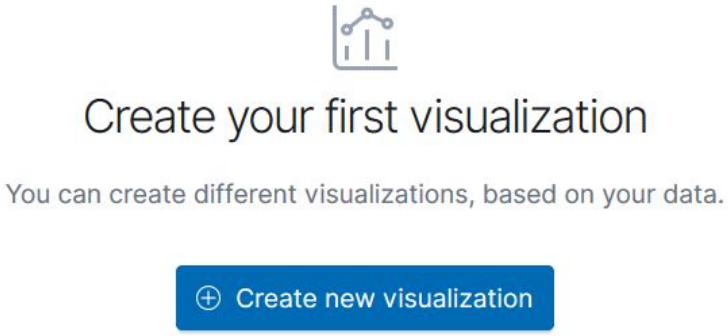
Ans: CmjiklOm3bnHgctw

Solution:

Step 1: Create a visualization to figure this out. Navigate to the 'Visualize' Section.



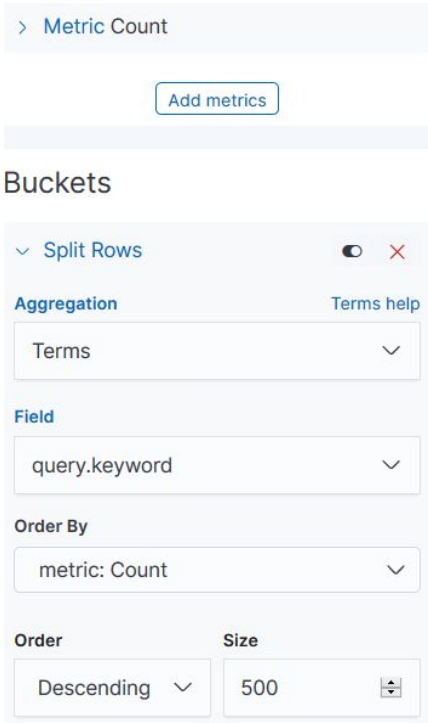
Step 2: Click on 'Create new visualization'.



Step 3: Select 'Data Table' Visualization.

Step 4: Choose the logstash-* index pattern as the source.

Step 5: Split the rows by applying 'Terms' aggregation on 'query.keyword' field.



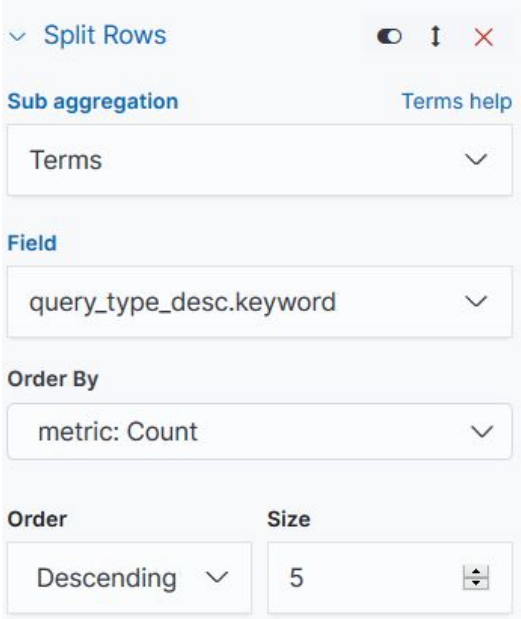
Step 6: Press the 'Apply changes' button.

query.keyword: Descending	Count
teredo.ipv6.microsoft.com	39,273
tools.google.com	14,057
www.apple.com	13,390
time.apple.com	13,109
safebrowsing.clients.google.com	11,658

Step 7: Select the zoom-into button for the sub-domain time.apple.com.

query.keyword: Descending	Count
time.apple.com	13,109

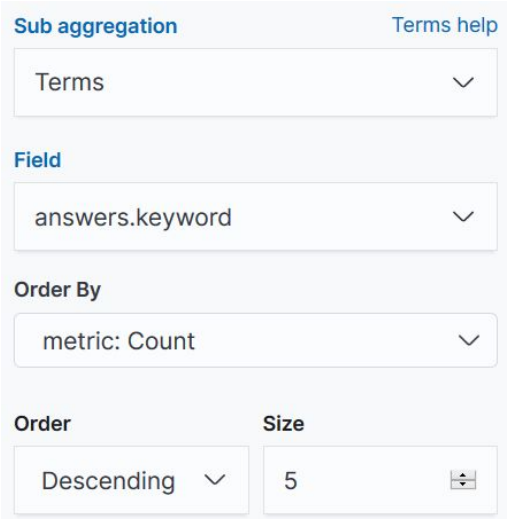
Step 8: Apply a 'Terms' sub-aggregation on the field 'query_type_desc.keyword'.



Step 8: Press the 'Apply changes' button.

query.keyword: Descending	query_type_desc.keyword: Descending	Count
time.apple.com	TXT	10,188
time.apple.com	AAAA	1,468
time.apple.com	A	1,453

Step 9: Apply a 'Terms' sub-aggregation on the field 'answers.keyword'.



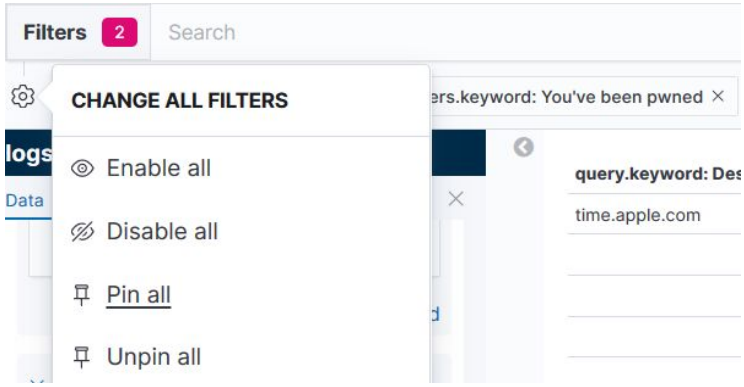
Step 10: Press the 'Apply changes' button.

query.keyword: Descending	query_type_desc.keyword: Descending	answers.keyword: Descending	Count
time.apple.com	TXT	-	10,187
time.apple.com	TXT	You've been pwned	1
time.apple.com	AAAA	-	1,468
time.apple.com	A	-	1,453

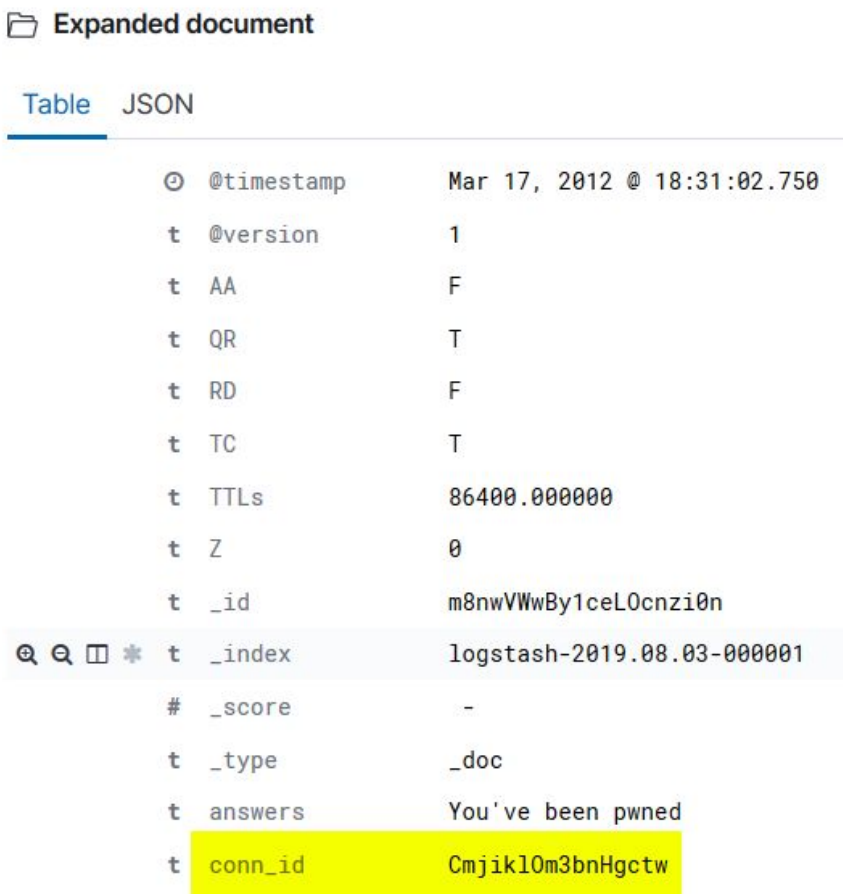
There was an entry containing the answer "You've been pwned". Zoom-into this answer entry.

query.keyword: Descending	query_type_desc.keyword: Descending	answers.keyword: Descending	Count
time.apple.com	TXT	You've been pwned	1

Step 11: Pin all the filters and navigate to the discover window.



Step 12: Retrieve the connection ID from the conn_id field.



The connection ID of that request was "CmjiklOm3bnHgctw".

References:

1. ELK Stack (https://www.elastic.co/elk-stack)
2. Log Source: http://www.secrepo.com/maccdc2012/dns.log.gz
   (Security Repo maintained by Mike Sconzo and licensed under Creative Commons Attribution 4.0 International License)