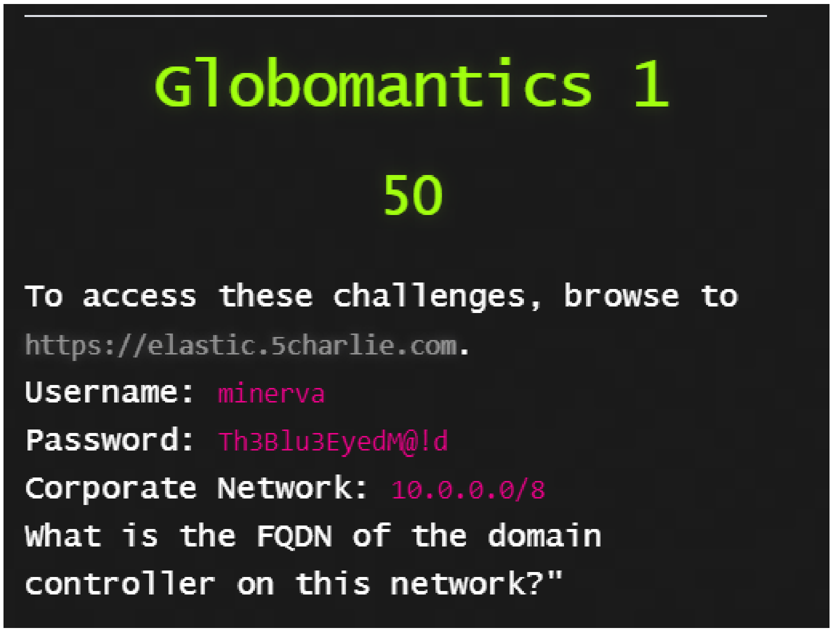


Globomantics 1

50

To access these challenges, browse to https://elastic.5charlie.com.

Username: minerva

Password: Th3Blu3EyedM@!d

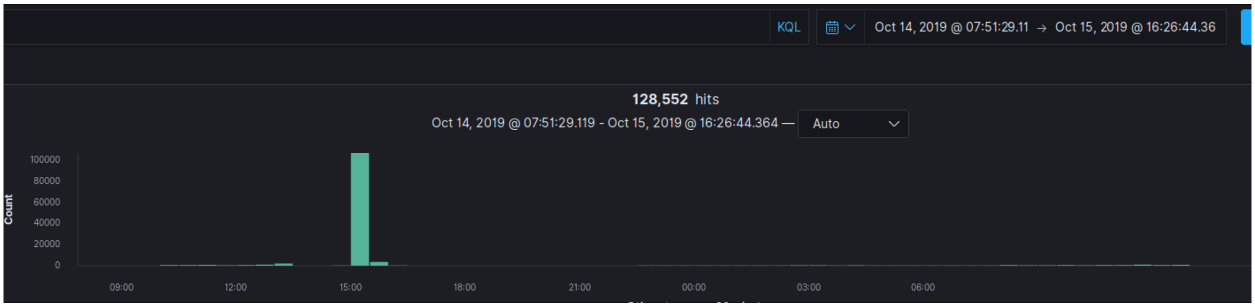
Corporate Network: 10.0.0.0/8

What is the FQDN of the domain controller on this network?"

Once we log in, we need to go to the discovery tab and find where the data is located.

Switch the time from last 15 min to last 3 years. From there we can zoom into the time by dragging the mouse over the area that has data

Data is from oct 15, 2019 to oct 16 ,2019

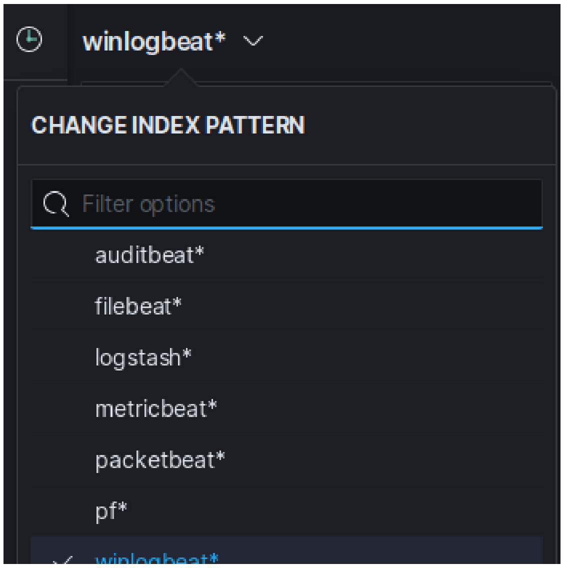


Oct 14, 2019 @ 07:51:29.11 → Oct 15, 2019 @ 16:26:44.36

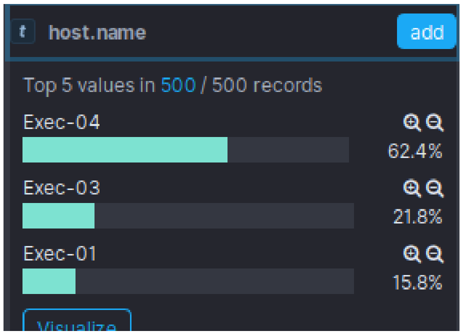
128,552 hits

Oct 14, 2019 @ 07:51:29.119 - Oct 15, 2019 @ 16:26:44.364 — Auto

We have a bunch of index patterns to choose from, but we want to look in the winlogbeat first as the dc is most likely a windows box.



If we look at the fields on the left-hand side, we can see that there may be one of interest to see if we have logs coming in from the dc itself is host.name

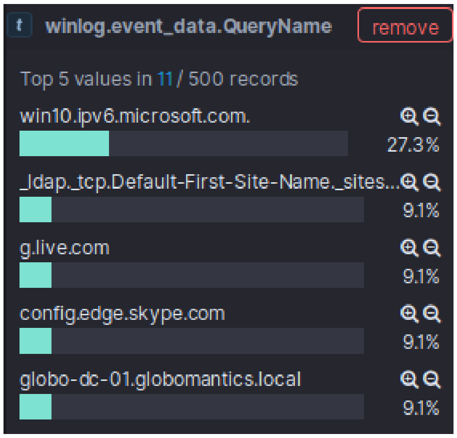


host.name

Top 5 values in 500 / 500 records

Exec-04 62.4%
Exec-03 21.8%
Exec-01 15.8%

So, we do not have a dc sending logs directly, but these 3 boxes have to query the dc somehow in order to validate credentials. There is a filed called winlon.event_data.QueryName that may give us an answer to this.

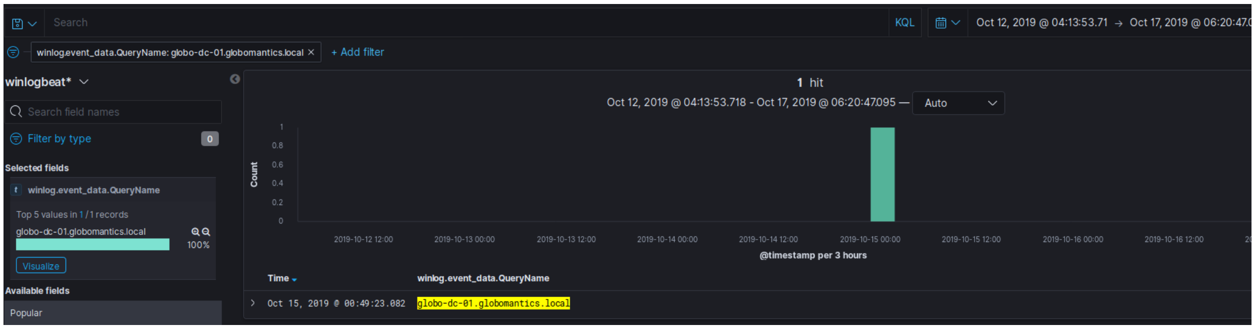


winlog.event_data.QueryName

Top 5 values in 11 / 500 records

win10.ipv6.microsoft.com. 27.3%
_ldap._tcp.Default-First-Site-Name._sites... 9.1%
g.live.com 9.1%
config.edge.skype.com 9.1%
globo-dc-01.globomantics.local 9.1%

We see the last one as a dc click the + sign next to this to filter to all the documents with that.



Oct 12, 2019 @ 04:13:53.71 → Oct 17, 2019 @ 06:20:47.0

winlog.event_data.QueryName: globo-dc-01.globomantics.local ×

winlog.event_data.QueryName

Top 5 values in 1 / 1 records

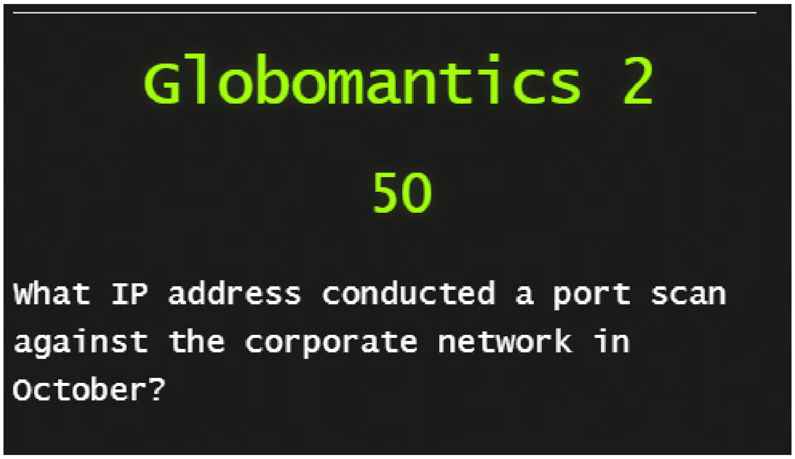
globo-dc-01.globomantics.local 100%

1 hit

Oct 12, 2019 @ 04:13:53.718 - Oct 17, 2019 @ 06:20:47.095 — Auto

```
  Time                        winlog.event_data.QueryName
> Oct 15, 2019 @ 00:49:23.082 globo-dc-01.globomantics.local
```

Flag: globo-dc-01.globomantics.local



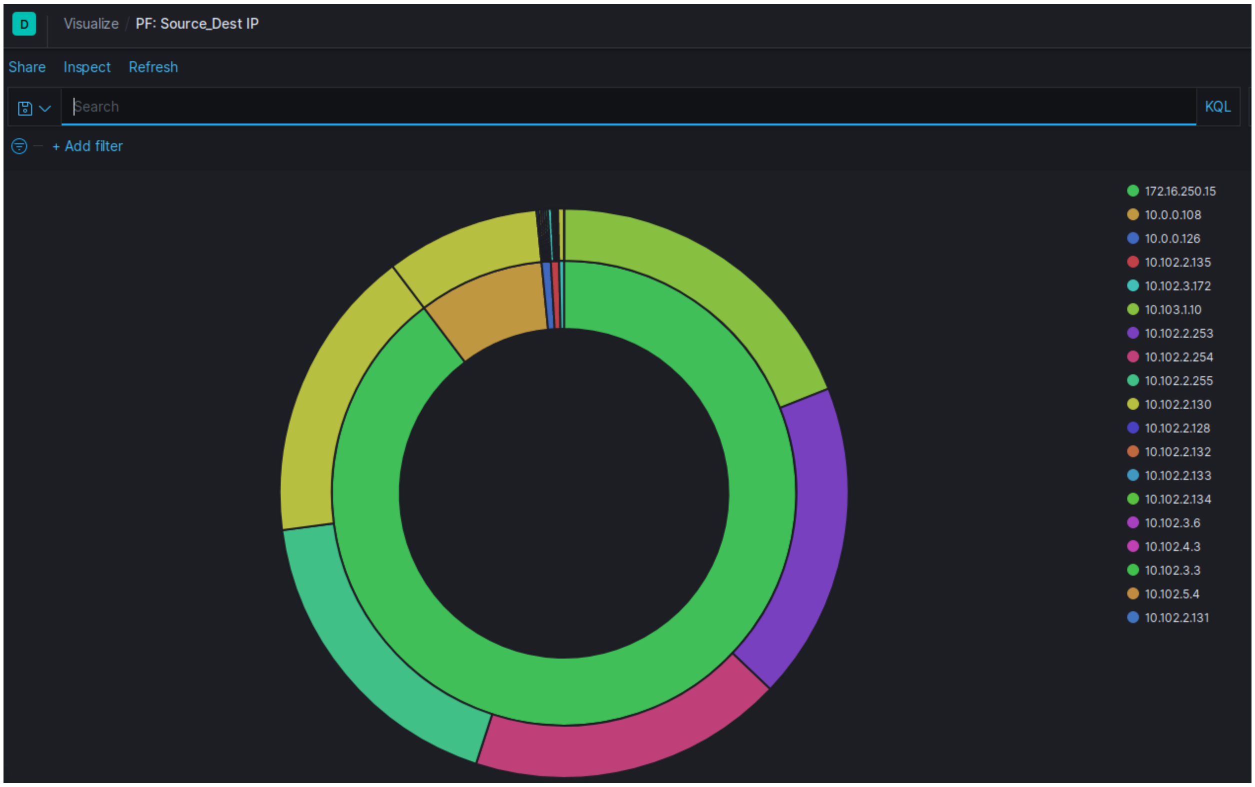
Globomantics 2

50

What IP address conducted a port scan against the corporate network in October?

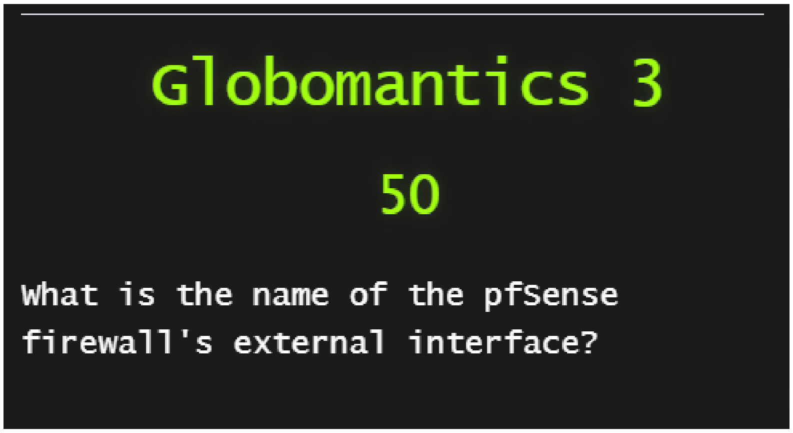
We will look at the pf index pattern as this is the firewall, we want to see who is talking to all the ips on our network.

We can look at the visualizations that are in Kibana for pf and the PF: Source_Dest IP looks interesting.



We can easily see that there is on ip not in our network talking to a lot of our systems

Flag: 172.16.250.15

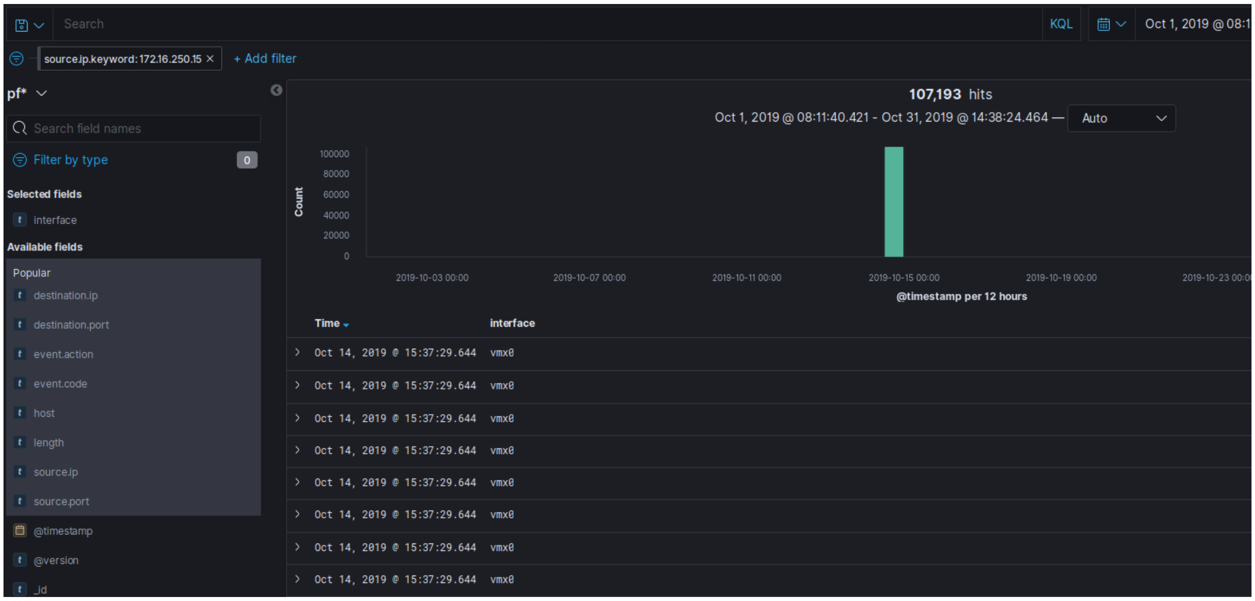


Globomantics 3

50

What is the name of the pfSense firewall's external interface?

We can filter on source.ip.keyword:172.16.250.15 in the pf index pattern, and we can add the interface column to see the answer.

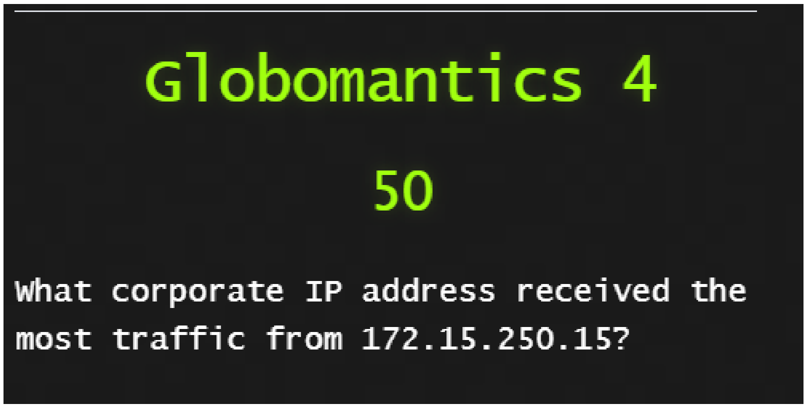


107,193 hits

Oct 1, 2019 @ 08:11:40.421 - Oct 31, 2019 @ 14:38:24.464 —

Time	interface
Oct 14, 2019 @ 15:37:29.644	vmx0
Oct 14, 2019 @ 15:37:29.644	vmx0
Oct 14, 2019 @ 15:37:29.644	vmx0
Oct 14, 2019 @ 15:37:29.644	vmx0
Oct 14, 2019 @ 15:37:29.644	vmx0
Oct 14, 2019 @ 15:37:29.644	vmx0
Oct 14, 2019 @ 15:37:29.644	vmx0
Oct 14, 2019 @ 15:37:29.644	vmx0

Flag: vmx0

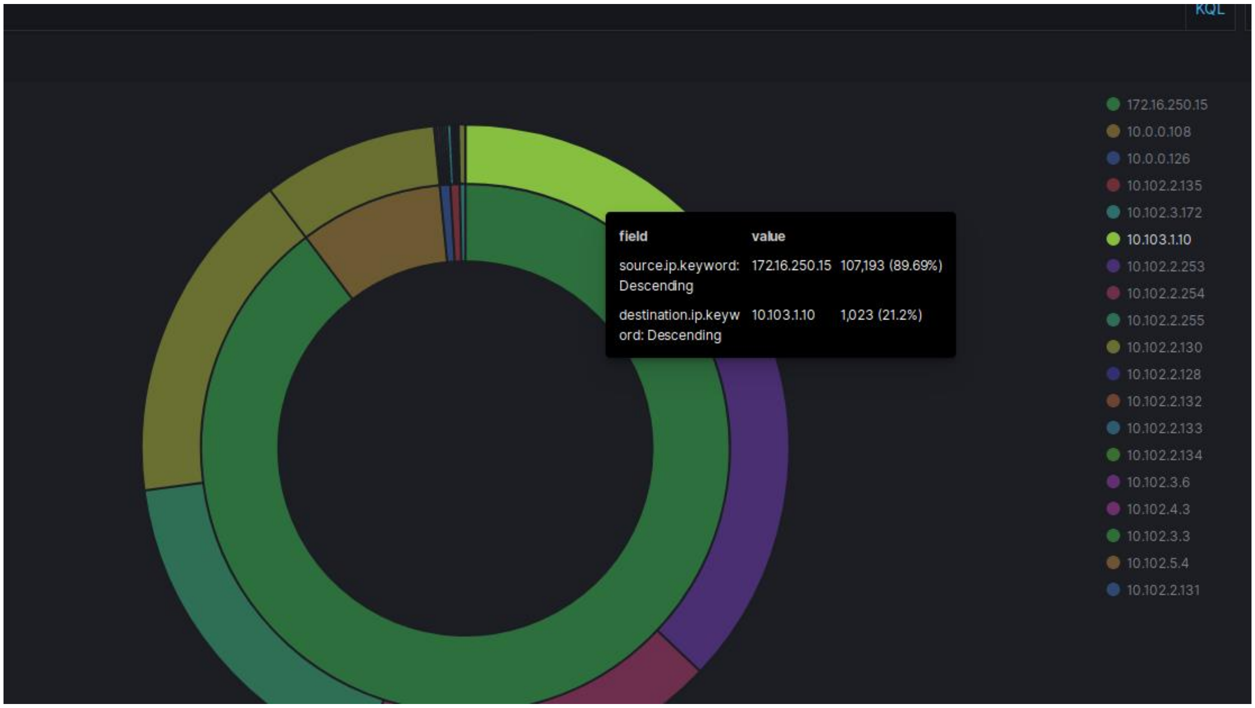


Globomantics 4

50

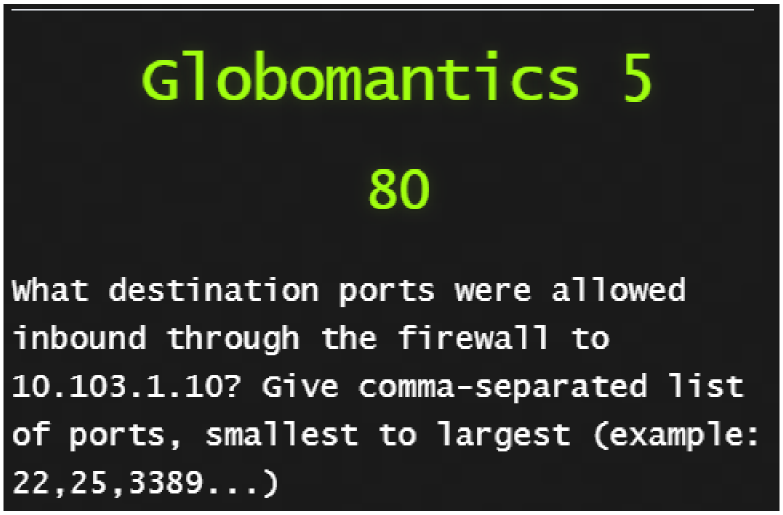
What corporate IP address received the most traffic from 172.15.250.15?

Going back to the PF: Source_Dest IP it is clear that 10.103.1.10 has the most traffic from that ip.



field	value	
source.ip.keyword: Descending	172.16.250.15	107,193 (89.69%)
destination.ip.keyword: Descending	10.103.1.10	1,023 (21.2%)

Flag: 10.103.1.10



Globomantics 5

80

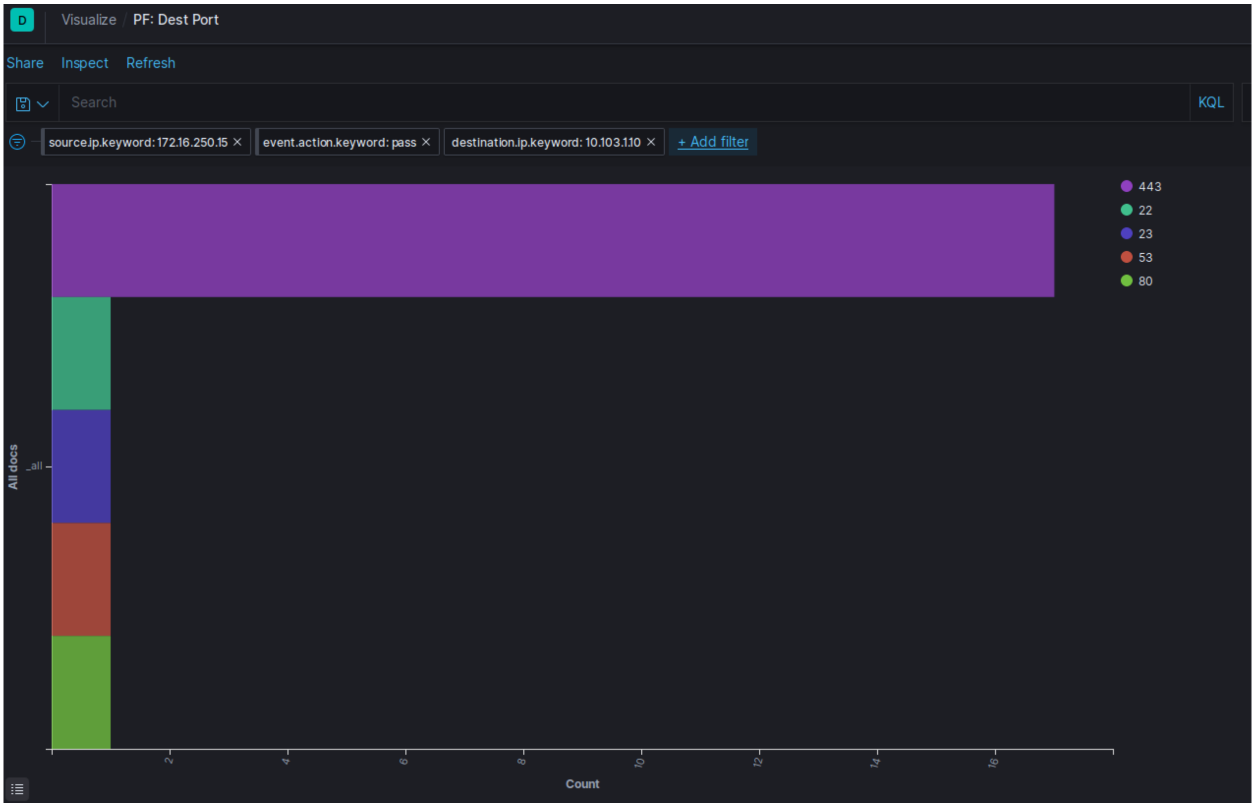
What destination ports were allowed inbound through the firewall to 10.103.1.10? Give comma-separated list of ports, smallest to largest (example: 22,25,3389...)

For this one we need to use the PF: Dest Port visual, but we need to limit it down with filters:

Source.ip.keyword: 172.16.250.15 - source of scan

Event.action.keyword: pass - allowed through firewall

Destication.ip.keywork: 10.103.1.10 - target of scan

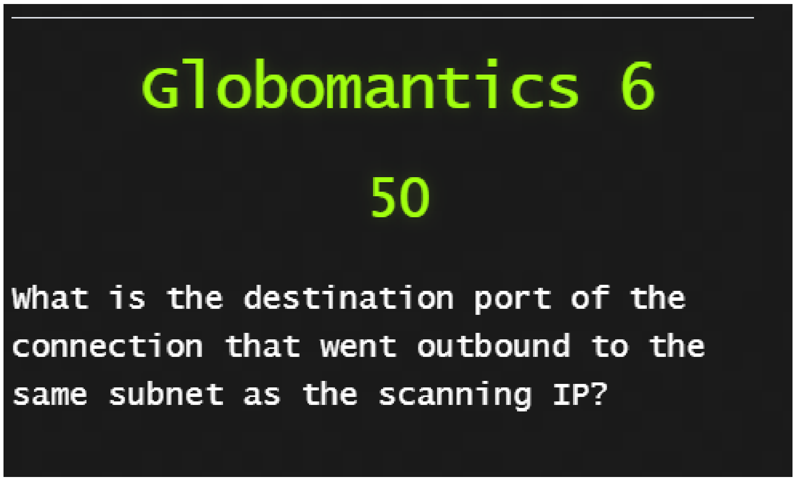


source.ip.keyword: 172.16.250.15

event.action.keyword: pass

destination.ip.keyword: 10.103.1.10

Flag: 22,23,53,80,443



Globomantics 6

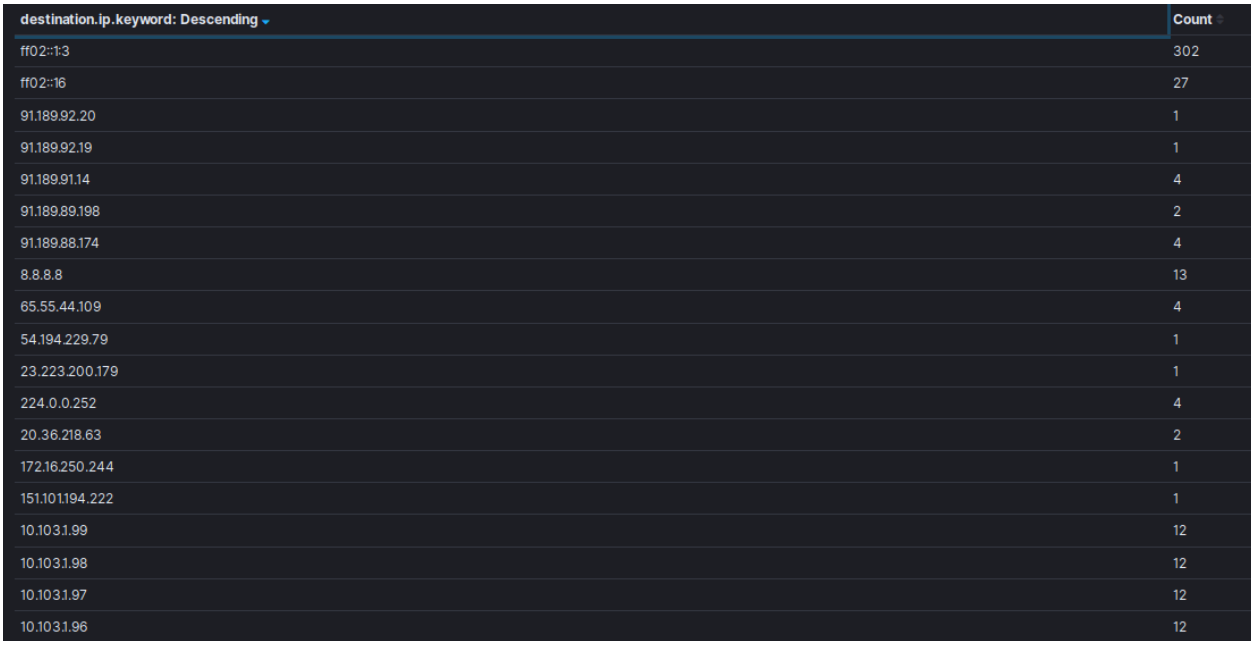
50

What is the destination port of the connection that went outbound to the same subnet as the scanning IP?

We can look for all destination ips that are in the 172.x.x.x subnet, in order to do this we can create a data table visual that will display all the terms in destination.ip.keyword.

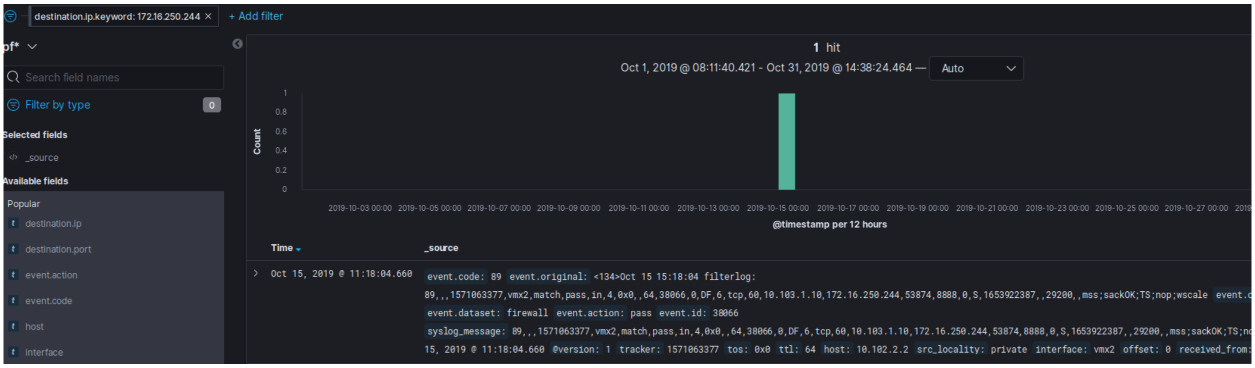
Bump up the size to very large number (5000) to make sure to grab all the ips.

Sort on the ip address until you get non 10.x.x.x as the first ip.



destination.ip.keyword: Descending	Count
ff02::1:3	302
ff02::16	27
91.189.92.20	1
91.189.92.19	1
91.189.91.14	4
91.189.89.198	2
91.189.88.174	4
8.8.8.8	13
65.55.44.109	4
54.194.229.79	1
23.223.200.179	1
224.0.0.252	4
20.36.218.63	2
172.16.250.244	1
151.101.194.222	1
10.103.1.99	12
10.103.1.98	12
10.103.1.97	12
10.103.1.96	12

We see that there is only one ip in the 172 Subnet: 172.16.250.244 that received traffic. We will pivot on this ip to discovery and find the port (pin to all apps to bring it across to discovery)

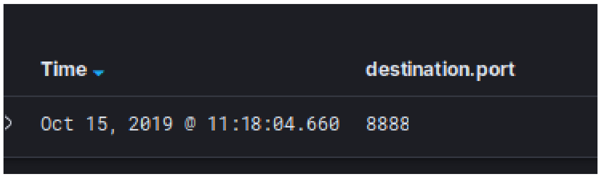


destination.ip.keyword: 172.16.250.244

1 hit

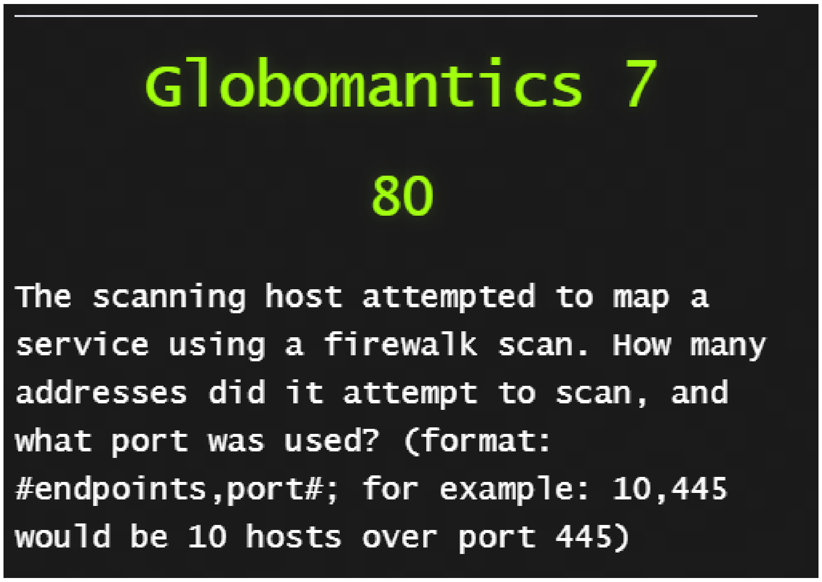
Oct 1, 2019 @ 08:11:40.421 - Oct 31, 2019 @ 14:38:24.464 —

```
Time                         _source
Oct 15, 2019 @ 11:18:04.660  event.code: 89 event.original: <134>Oct 15 15:18:04 filterlog:
                             89,,,1571063377,vmx2,match,pass,in,4,0x0,,64,38066,0,DF,6,tcp,60,10.103.1.10,172.16.250.244,53874,8888,0,S,1653922387,,29200,,mss;sackOK;TS;nop;wscale event.c
                             event.dataset: firewall event.action: pass event.id: 38066
                             syslog_message: 89,,,1571063377,vmx2,match,pass,in,4,0x0,,64,38066,0,DF,6,tcp,60,10.103.1.10,172.16.250.244,53874,8888,0,S,1653922387,,29200,,mss;sackOK;TS;no
                             15, 2019 @ 11:18:04.660 @version: 1 tracker: 1571063377 tos: 0x0 ttl: 64 host: 10.102.2.2 src_locality: private interface: vmx2 offset: 0 received_from:
```



Time	destination.port
Oct 15, 2019 @ 11:18:04.660	8888

Flag: 8888



Globomantics 7

80

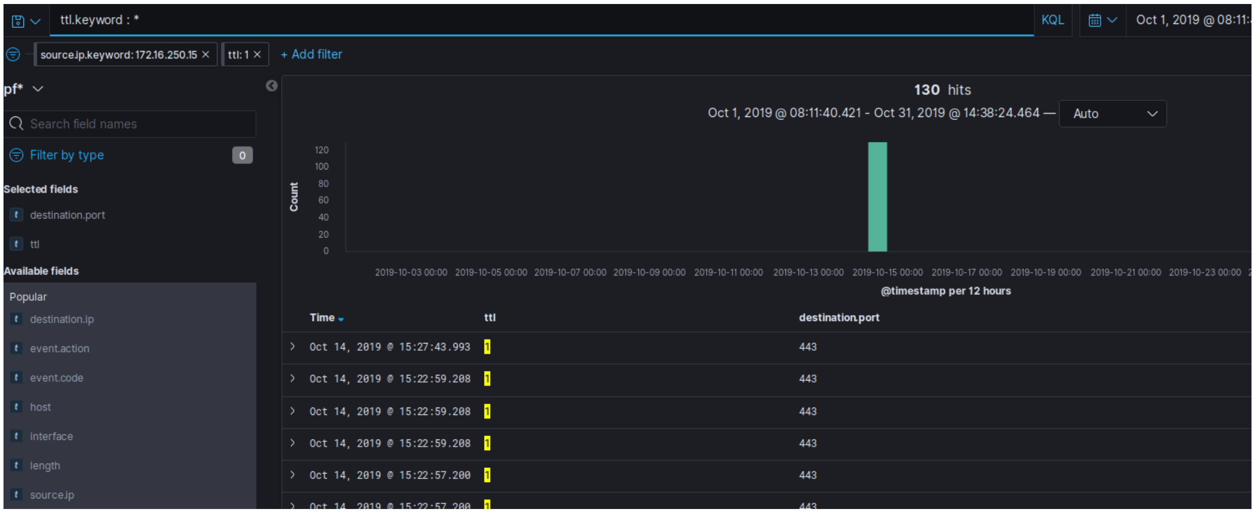
The scanning host attempted to map a service using a firewalk scan. How many addresses did it attempt to scan, and what port was used? (format: #endpoints,port#; for example: 10,445 would be 10 hosts over port 445)

Here is a definition of firewalking: Developed by Mike Schiffman and David Goldsmith, a technique for testing the vulnerability of a firewall and mapping the routers of a network that sits behind a firewall. Firewalking is a method of disguising port scans. In practical applications, firewalking is similar to tracerouting and works by sending into the firewall TCP or UDP packets that have a TTL set at one hop greater than the targeted firewall. If the packet makes it through the gateway, it is forwarded to the next hop where the TTL equals zero and elicits a TTL "exceeded in transit" message, at which point the packet is discarded. Using this method, access information on the firewall can be determined if successive probe packets are sent.

So, the key here will be finding that ttl: 1 as a filter

In discovery if we put in the filter for source.ip.keyword: 172.16.250.15 and ttl: 1

We see that there is a bunch of results that show us our answer.



ttl.keyword : *

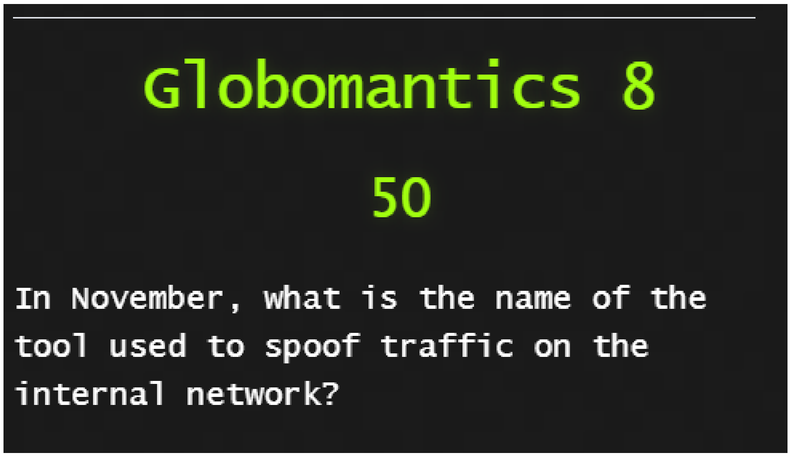
source.ip.keyword: 172.16.250.15 ttl: 1

130 hits

Oct 1, 2019 @ 08:11:40.421 - Oct 31, 2019 @ 14:38:24.464 — Auto

Time	ttl	destination.port
Oct 14, 2019 @ 15:27:43.993	1	443
Oct 14, 2019 @ 15:22:59.208	1	443
Oct 14, 2019 @ 15:22:59.208	1	443
Oct 14, 2019 @ 15:22:59.208	1	443
Oct 14, 2019 @ 15:22:57.200	1	443
Oct 14, 2019 @ 15:22:57.200	1	443

Flag: 130,443



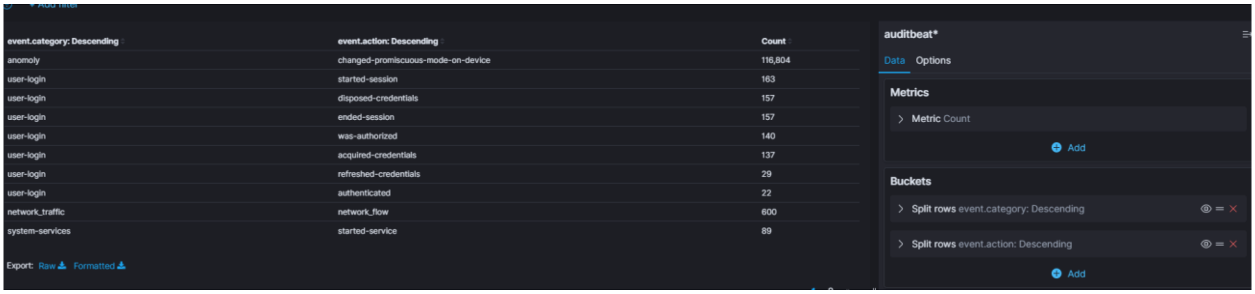
Globomantics 8

50

In November, what is the name of the tool used to spoof traffic on the internal network?

We want to look at the data for auditbeat during the November timeframe. After looking at the data points there is an event.category and event.action

We car create a visualization on these two fields to see if there is anything of interest here.



event.category: Descending	event.action: Descending	Count
anomoly	changed-promiscuous-mode-on-device	116,804
user-login	started-session	163
user-login	disposed-credentials	157
user-login	ended-session	157
user-login	was-authorized	140
user-login	acquired-credentials	137
user-login	refreshed-credentials	29
user-login	authenticated	22
network_traffic	network_flow	600
system-services	started-service	89

Export: Raw Formatted

auditbeat*

Data Options

Metrics

Metric Count

Add

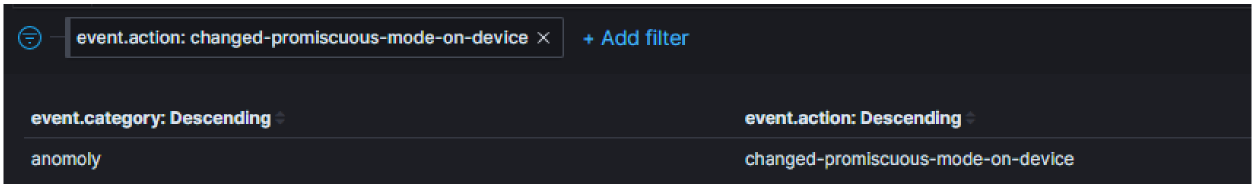
Buckets

Split rows event.category: Descending

Split rows event.action: Descending

Add

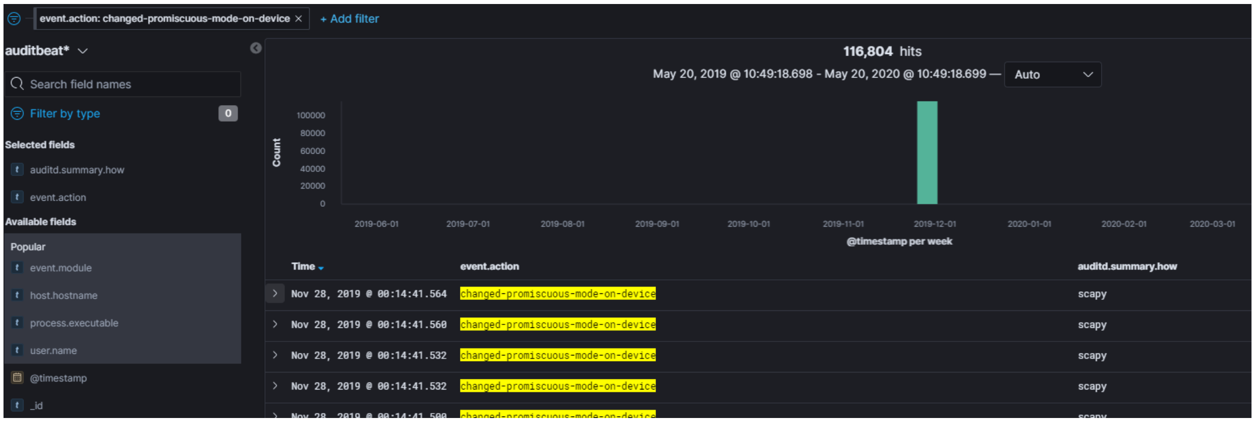
We see that there is an anomaly at the top and the action is promiscuous mode on device. This is done when spoofing or sniffing tools on a network are done. We will pivot from that event.action over to discovery to take a closer look.



event.action: changed-promiscuous-mode-on-device

event.category: Descending	event.action: Descending
anomoly	changed-promiscuous-mode-on-device

Here we can see under the auditd.summary.how that our answer is in front of us.

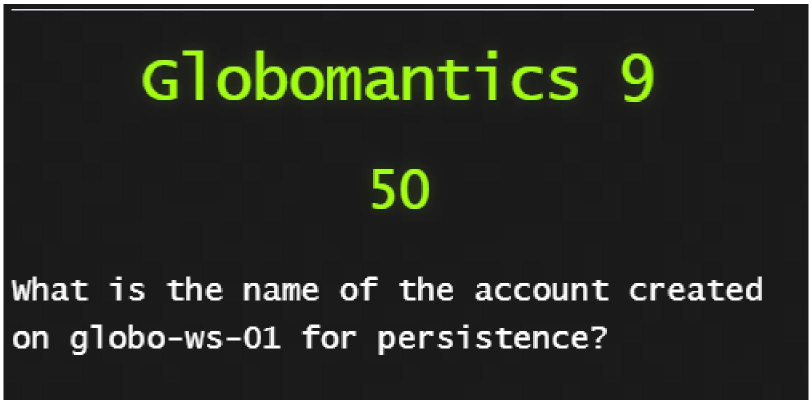


116,804 hits

May 20, 2019 @ 10:49:18.698 - May 20, 2020 @ 10:49:18.699 — Auto

Time	event.action	auditd.summary.how
Nov 28, 2019 @ 00:14:41.564	changed-promiscuous-mode-on-device	scapy
Nov 28, 2019 @ 00:14:41.560	changed-promiscuous-mode-on-device	scapy
Nov 28, 2019 @ 00:14:41.532	changed-promiscuous-mode-on-device	scapy
Nov 28, 2019 @ 00:14:41.532	changed-promiscuous-mode-on-device	scapy
Nov 28, 2019 @ 00:14:41.500	changed-promiscuous-mode-on-device	scapy

Flag: scapy



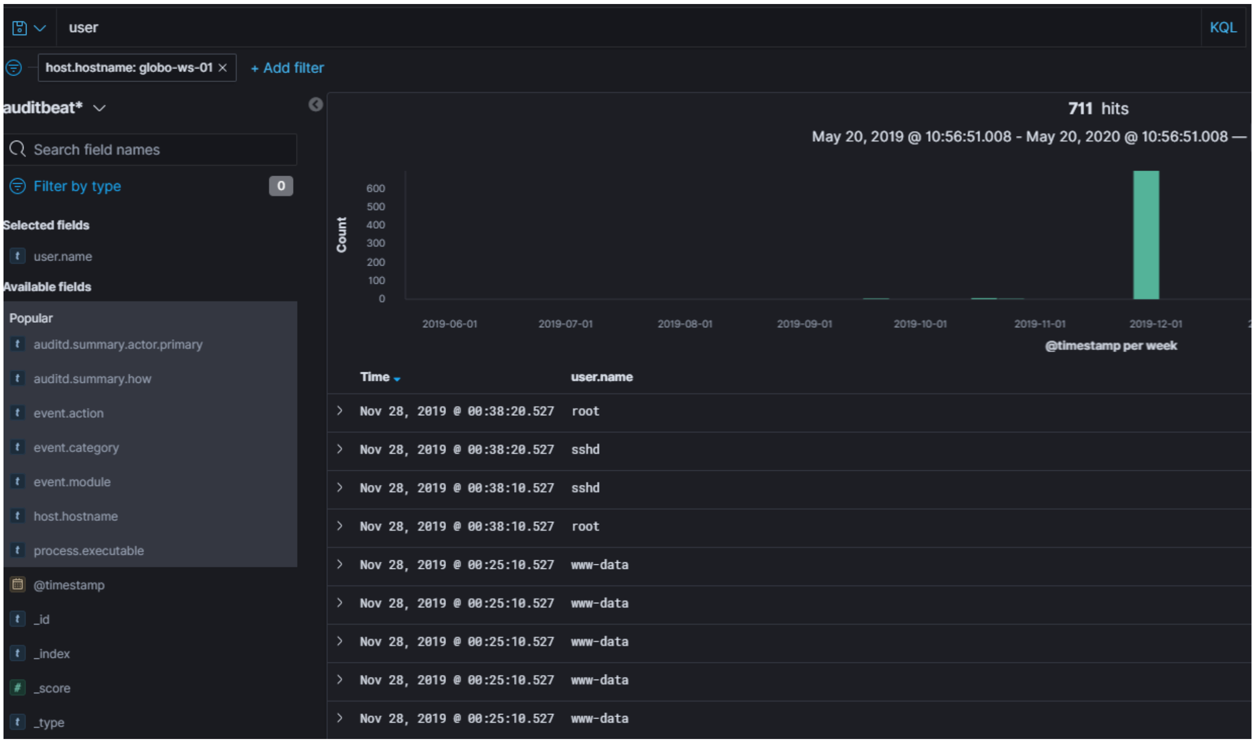
Globomantics 9

50

What is the name of the account created on globo-ws-01 for persistence?

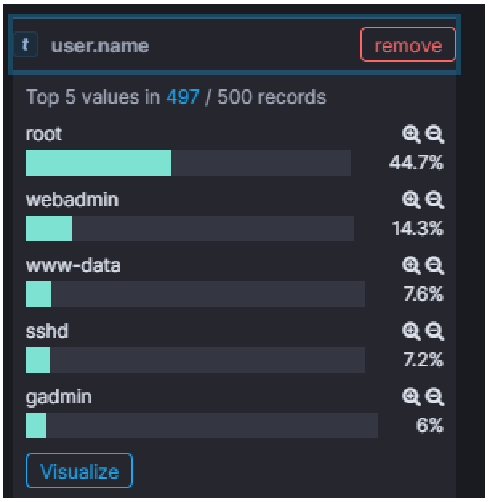
We need to create a filter on the auditbeat logs first to look at only the host.hostname: globo-ws-01

The field we are most likely interested in is the user.name field. We need to filter out the known correct accounts to find the possible bad accounts.



Time	user.name
Nov 28, 2019 @ 00:38:20.527	root
Nov 28, 2019 @ 00:38:20.527	sshd
Nov 28, 2019 @ 00:38:10.527	sshd
Nov 28, 2019 @ 00:38:10.527	root
Nov 28, 2019 @ 00:25:10.527	www-data
Nov 28, 2019 @ 00:25:10.527	www-data
Nov 28, 2019 @ 00:25:10.527	www-data
Nov 28, 2019 @ 00:25:10.527	www-data
Nov 28, 2019 @ 00:25:10.527	www-data

We can do a quick look at the user.name field and can see that after root there is another admin account or two on the box. We saw that gadmin was running the scappy program in question 8, but that was not the answer for 9.

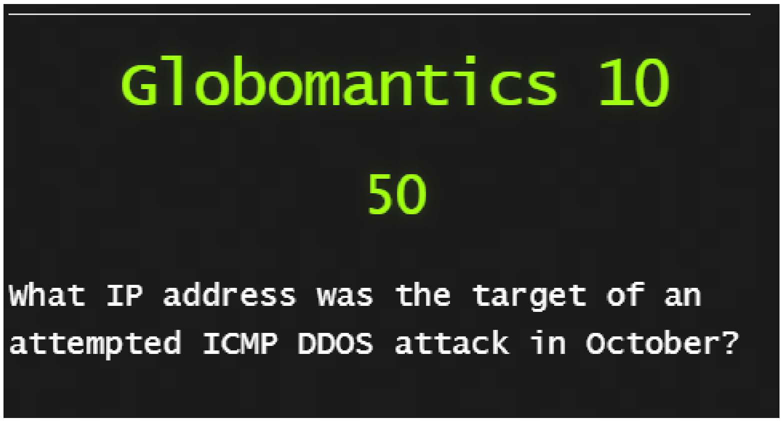


Top 5 values in 497 / 500 records

root	44.7%
webadmin	14.3%
www-data	7.6%
sshd	7.2%
gadmin	6%

www-data is the chrooted web server and sshd allows remote access via a service and neither of those should be admin accounts.

Flag: webadmin

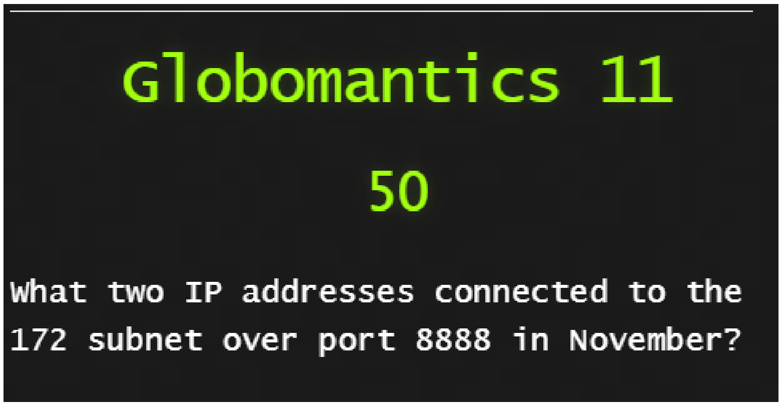


Globomantics 10

50

What IP address was the target of an attempted ICMP DDOS attack in October?

Currently not solvable with Grok Parse Failure

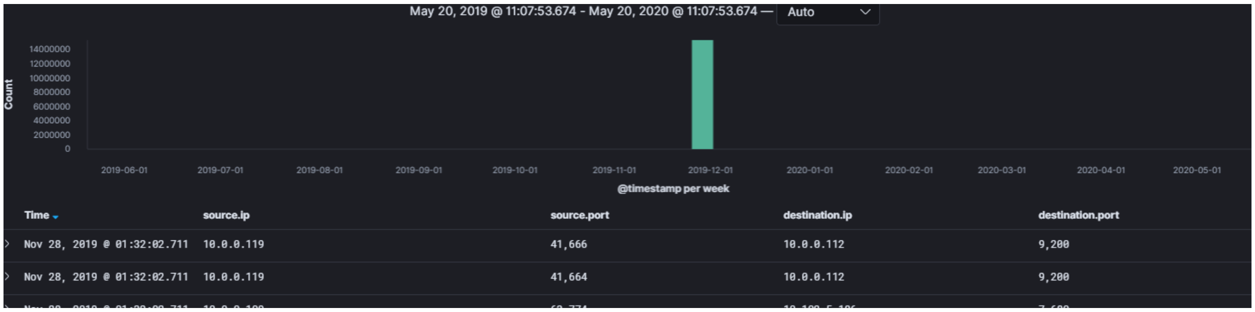


Globomantics 11

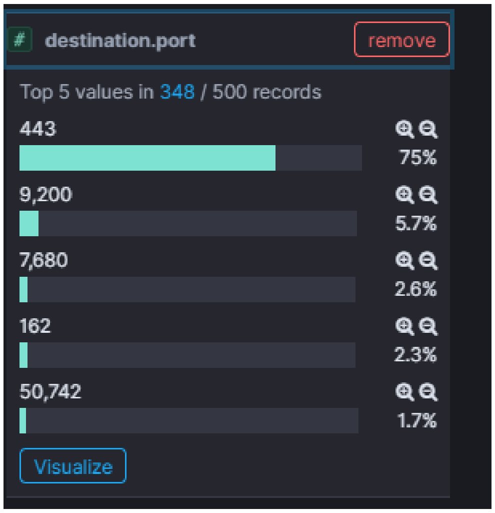
50

What two IP addresses connected to the 172 subnet over port 8888 in November?

Under that Packetbeat index pattern we are going to look at the destination.port in a visualization:

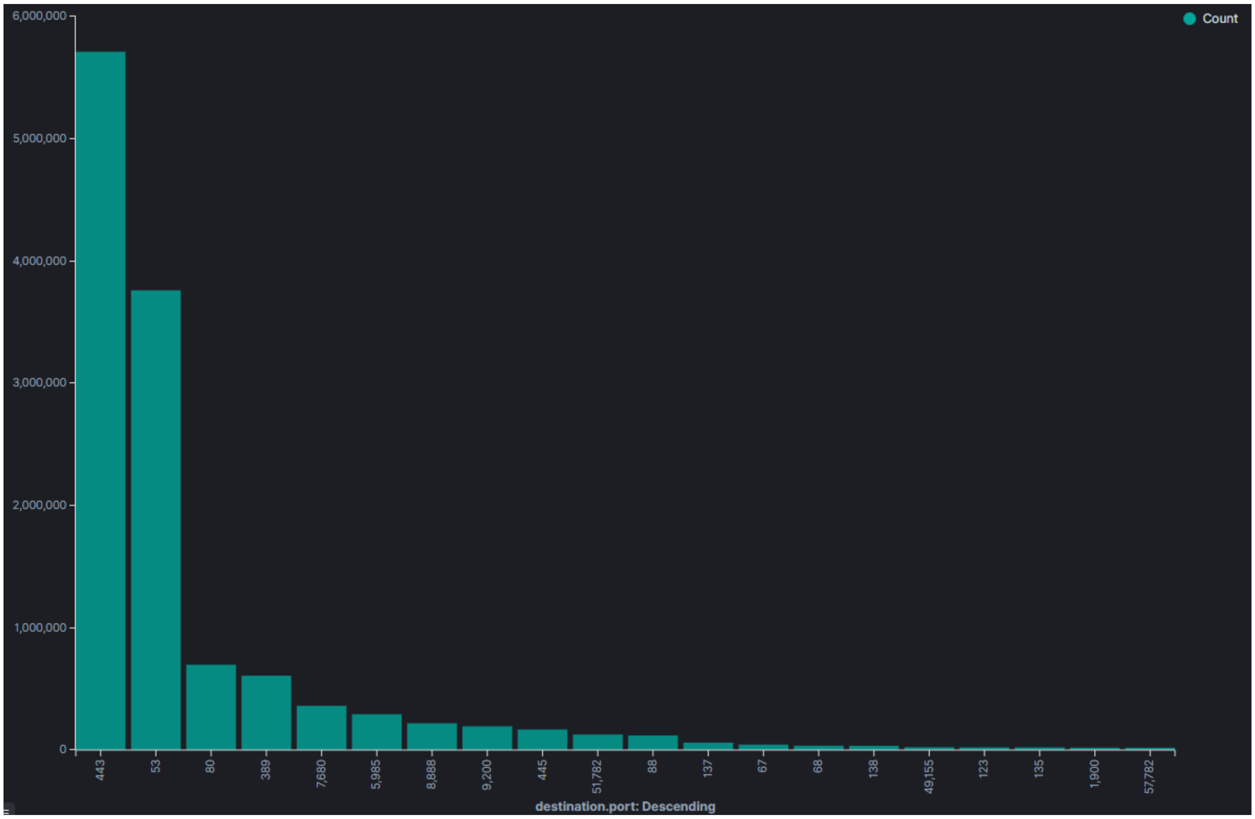


Time	source.ip	source.port	destination.ip	destination.port
Nov 28, 2019 @ 01:32:02.711	10.0.0.119	41,666	10.0.0.112	9,200
Nov 28, 2019 @ 01:32:02.711	10.0.0.119	41,664	10.0.0.112	9,200

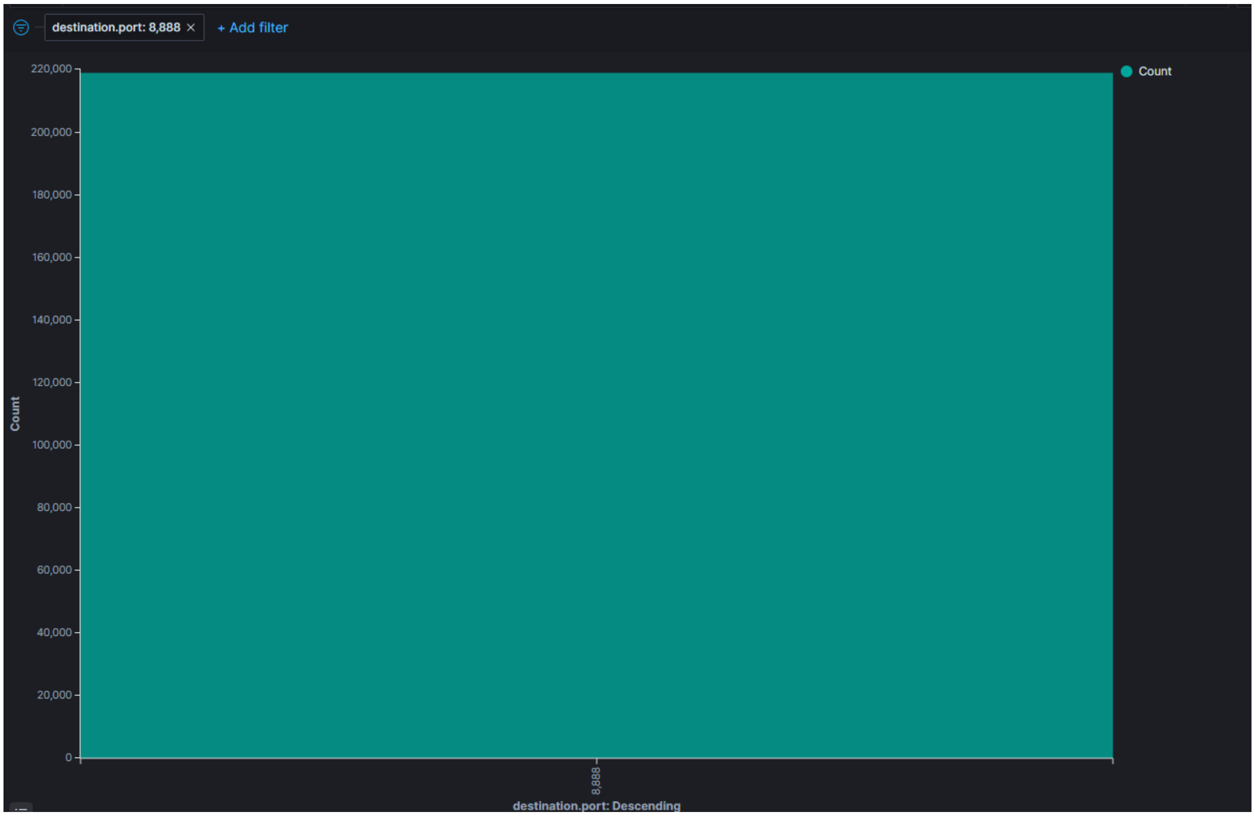


Top 5 values in 348 / 500 records

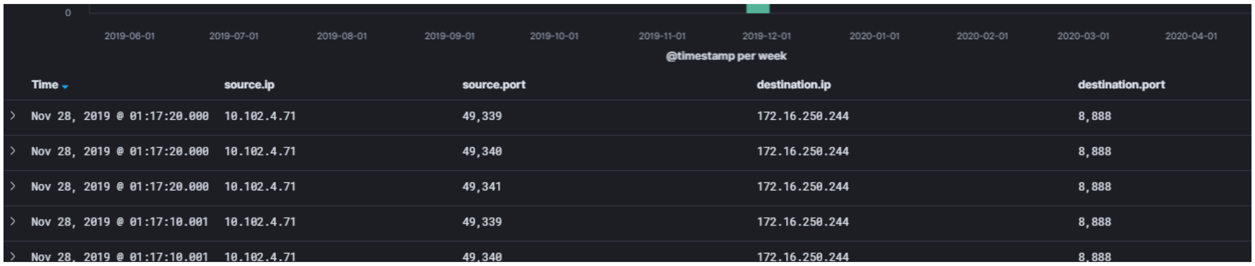
443	75%
9,200	5.7%
7,680	2.6%
162	2.3%
50,742	1.7%



Click on the port 8888

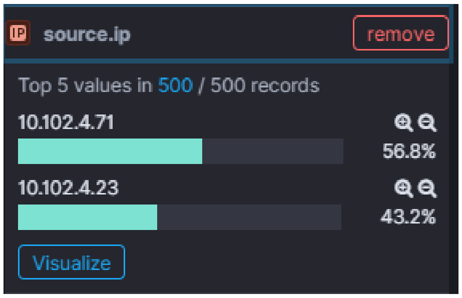


Pin the filter and go back to discovery



Time	source.ip	source.port	destination.ip	destination.port
Nov 28, 2019 @ 01:17:20.000	10.102.4.71	49,339	172.16.250.244	8,888
Nov 28, 2019 @ 01:17:20.000	10.102.4.71	49,340	172.16.250.244	8,888
Nov 28, 2019 @ 01:17:20.000	10.102.4.71	49,341	172.16.250.244	8,888
Nov 28, 2019 @ 01:17:10.001	10.102.4.71	49,339	172.16.250.244	8,888
Nov 28, 2019 @ 01:17:10.001	10.102.4.71	49,340	172.16.250.244	8,888

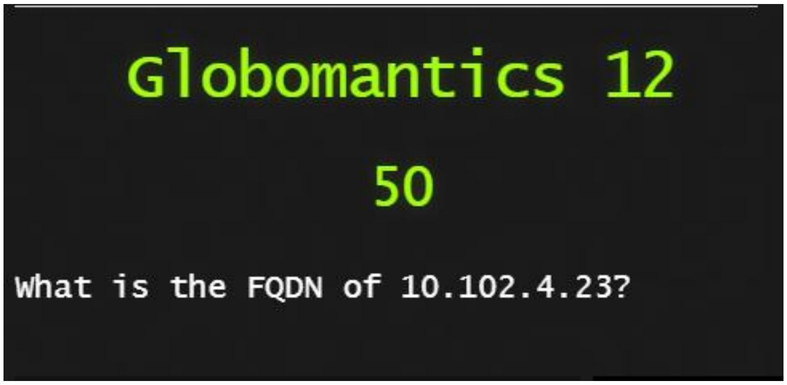
we can look at the source.ip field to find our two answers



Top 5 values in 500 / 500 records

10.102.4.71	56.8%
10.102.4.23	43.2%

Flag: 10.102.4.71,10.102.4.23

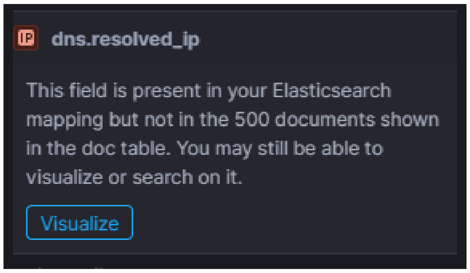


Globomantics 12

50

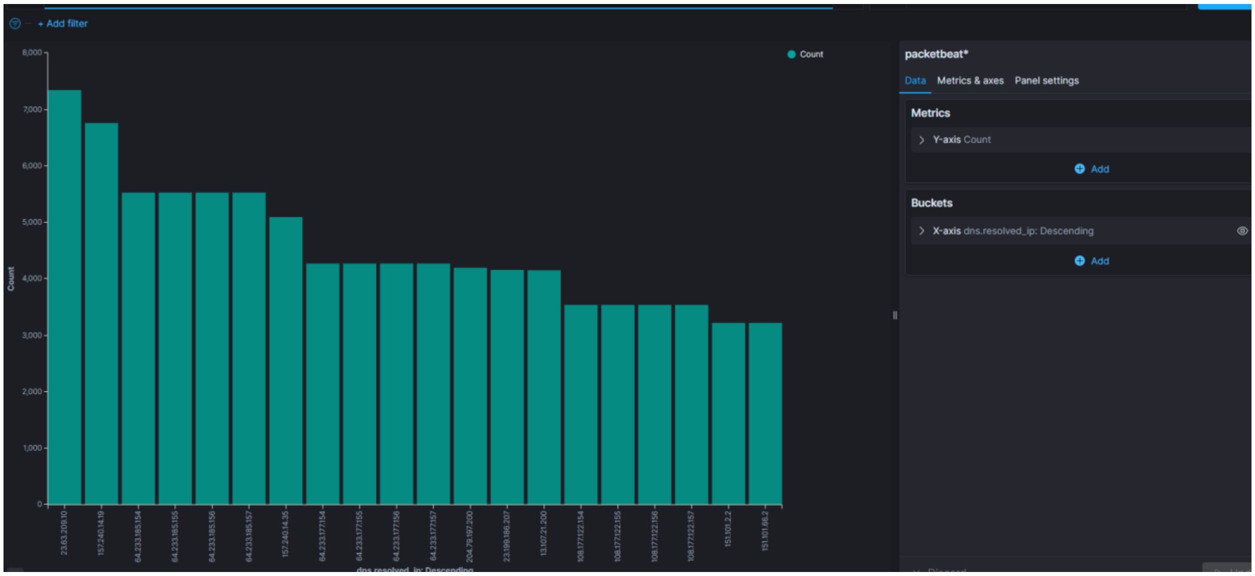
What is the FQDN of 10.102.4.23?

In packetbeat we want to look at the dns queries and in this case the dns.resolved_ip since there are over 15m packets the visual will be empty, but we will click on visualize it.

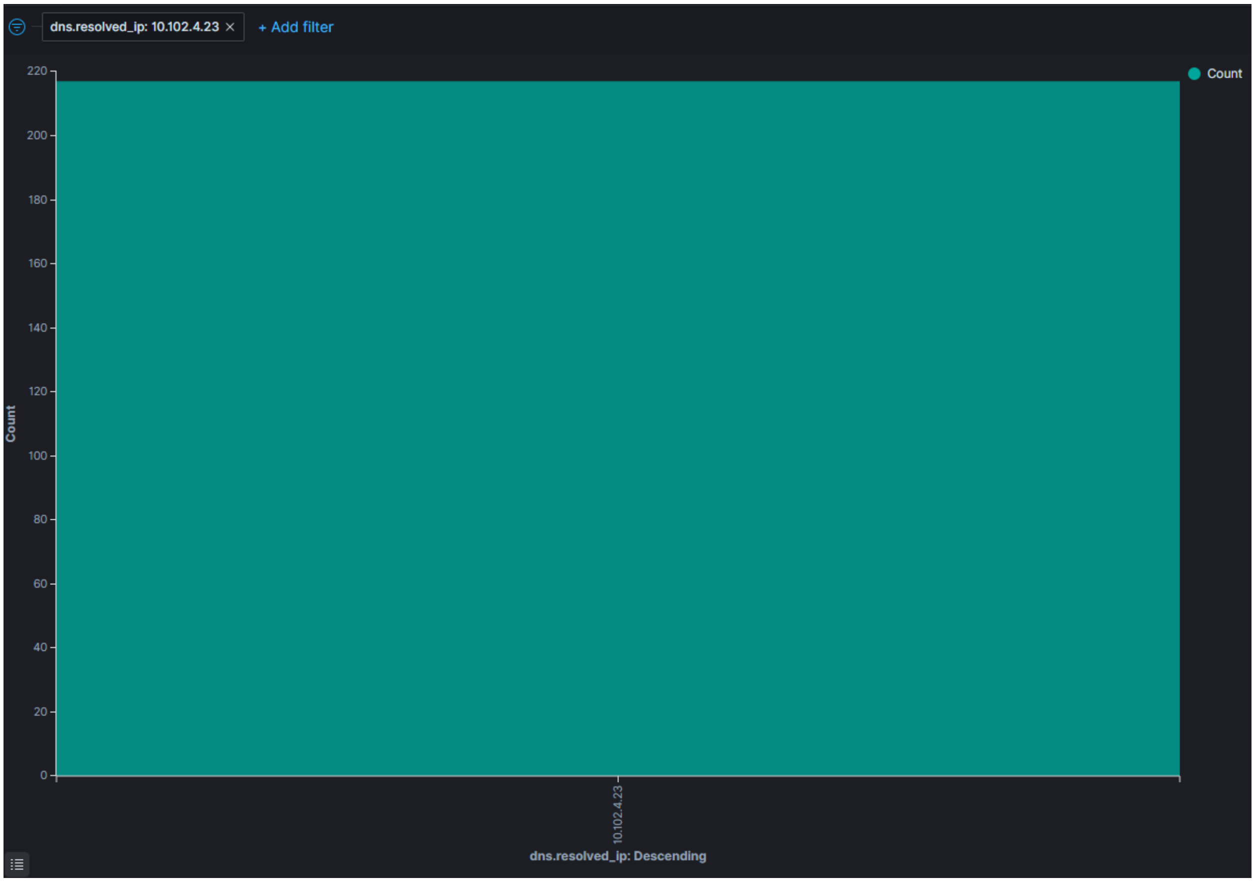


IP dns.resolved_ip

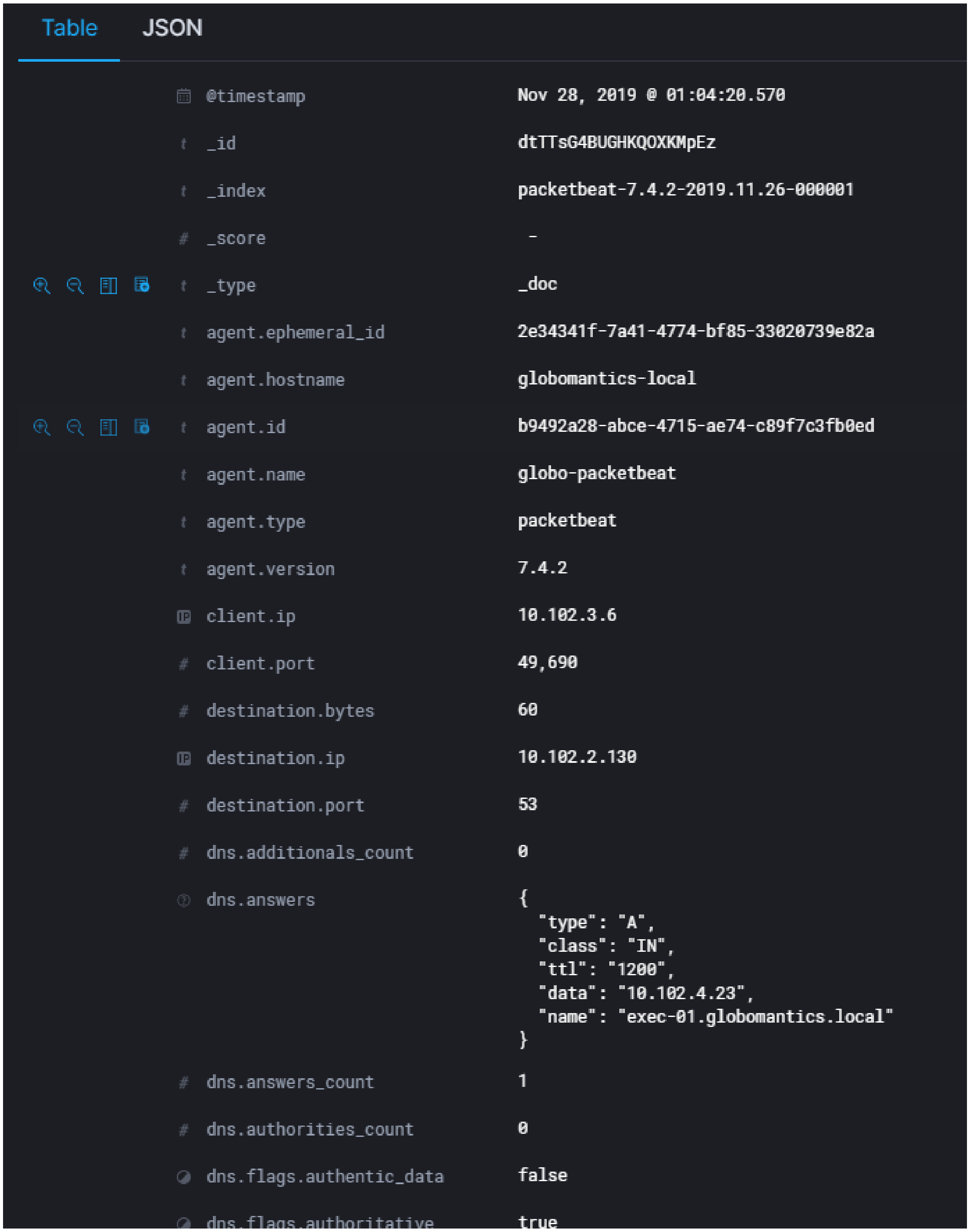
This field is present in your Elasticsearch mapping but not in the 500 documents shown in the doc table. You may still be able to visualize or search on it.



Click on one of the ip addresses and edit the filter to out IP address and when we confirm that we have some data there then pin and pivot to discovery.

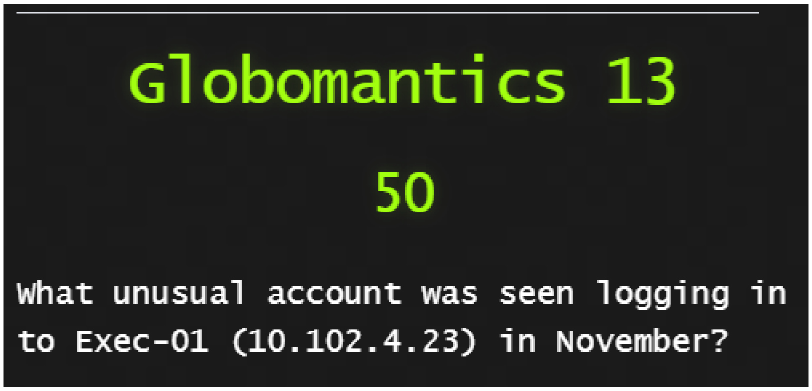


We can look at the document and see the dns.answers has what we are looking for.



```
@timestamp                Nov 28, 2019 @ 01:04:20.570
_id                       dtTTsG4BUGHKQOXKMpEz
_index                    packetbeat-7.4.2-2019.11.26-000001
_score                     -
_type                     _doc
agent.ephemeral_id        2e34341f-7a41-4774-bf85-33020739e82a
agent.hostname            globomantics-local
agent.id                  b9492a28-abce-4715-ae74-c89f7c3fb0ed
agent.name                globo-packetbeat
agent.type                packetbeat
agent.version             7.4.2
client.ip                 10.102.3.6
client.port               49,690
destination.bytes         60
destination.ip            10.102.2.130
destination.port          53
dns.additionals_count     0
dns.answers               {
                            "type": "A",
                            "class": "IN",
                            "ttl": "1200",
                            "data": "10.102.4.23",
                            "name": "exec-01.globomantics.local"
                          }
dns.answers_count         1
dns.authorities_count     0
dns.flags.authentic_data  false
dns.flags.authoritative   true
```

Flag: exec-01.globomantics.local

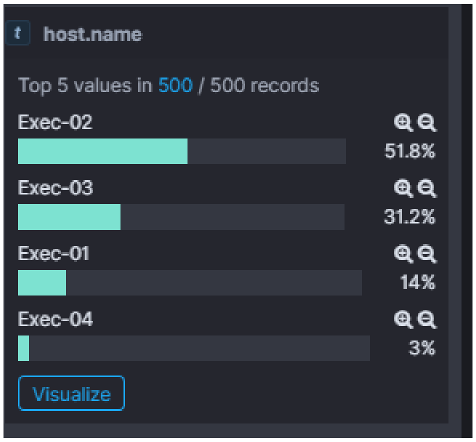


Globomantics 13

50

What unusual account was seen logging in to Exec-01 (10.102.4.23) in November?

We want to look at the winlogbeat data now and make sure that we are looking at exec-01 only for this first.



t host.name

Top 5 values in 500 / 500 records

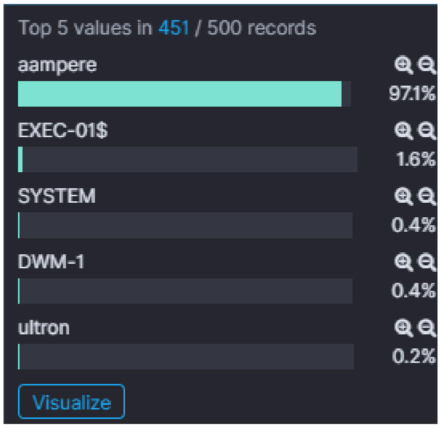
Exec-02 51.8%

Exec-03 31.2%

Exec-01 14%

Exec-04 3%

Once we have filtered on the exec-01 user we want to move over to see all the accounts that accessed the computer.



Top 5 values in 451 / 500 records

aampere 97.1%

EXEC-01$ 1.6%

SYSTEM 0.4%

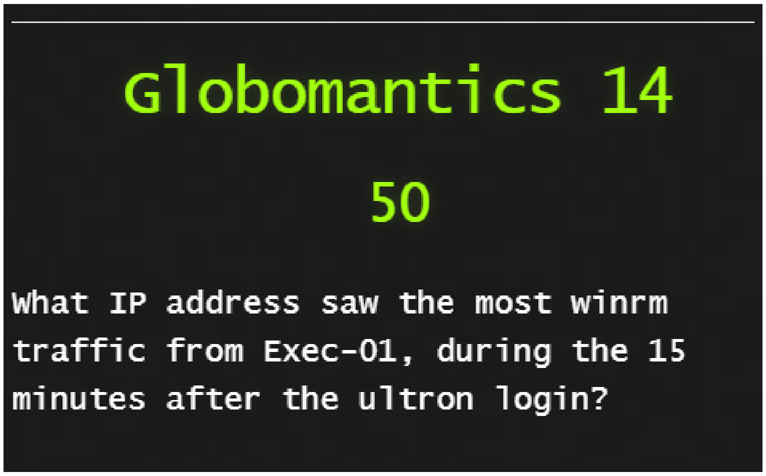
DWM-1 0.4%

ultron 0.2%

EXEC-01$ is a service account, system is local, DWM-1 is common windows management, and aampere is most likely the user.

Ultron does not fit here with this analysis.

Flag: Ultron

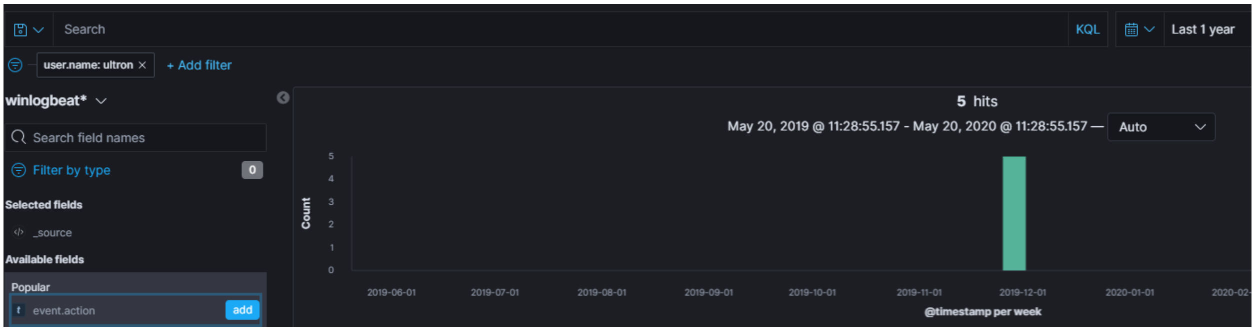


Globomantics 14

50

What IP address saw the most winrm traffic from Exec-01, during the 15 minutes after the ultron login?

We need to filter on the user Ultron to see the results of what they did.



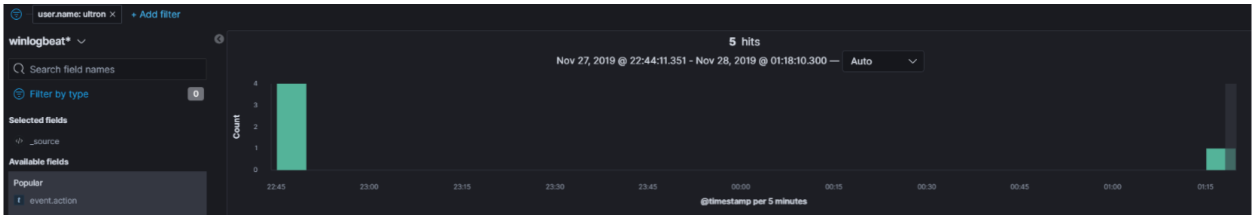
user.name: ultron

winlogbeat*

5 hits

May 20, 2019 @ 11:28:55.157 - May 20, 2020 @ 11:28:55.157 — Auto

With only 5 documents we should be able to find this answer, but what we need to look at is the timeframe of this as it seems that ultron has found their way into EXEC-01$ account for privilege escalation. We need to look at the winrm traffic that happens between Nov 27 @ 2245 to Nov 28 @ 0118



user.name: ultron

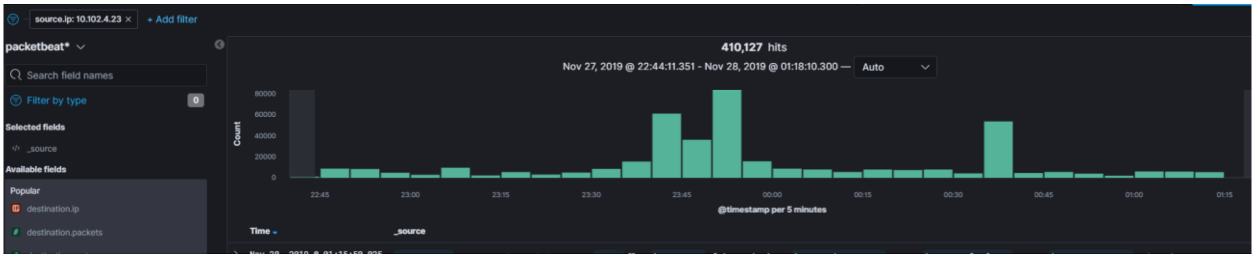
winlogbeat*

5 hits

Nov 27, 2019 @ 22:44:11.351 - Nov 28, 2019 @ 01:18:10.300 — Auto

We can switch over to packetbeat with this new time range selected still and look for any winrm going on.

We specifically want to look at the traffic from source.ip: 10.102.4.23

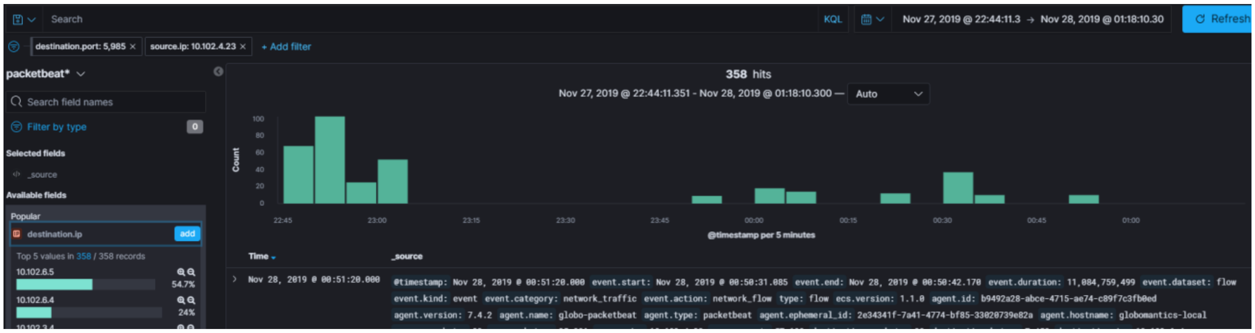


source.ip: 10.102.4.23

410,127 hits

Nov 27, 2019 @ 22:44:11.351 - Nov 28, 2019 @ 01:18:10.300 — Auto

Next we want to see only traffic with winrm, so look at destination.port and we want to filter on 5985.



Nov 27, 2019 @ 22:44:11.3 → Nov 28, 2019 @ 01:18:10.30

destination.port: 5,985 source.ip: 10.102.4.23

358 hits

Nov 27, 2019 @ 22:44:11.351 - Nov 28, 2019 @ 01:18:10.300 — Auto

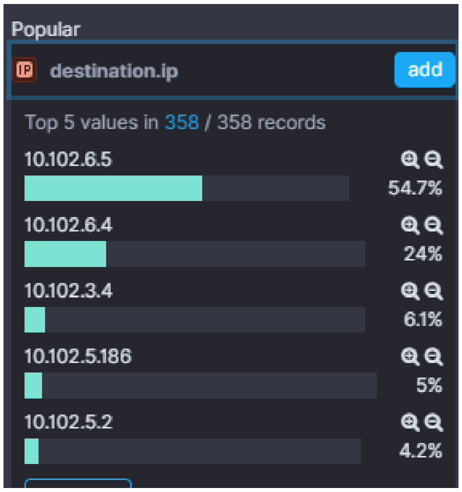
Top 5 values in 358 / 358 records

10.102.6.5 54.7%

10.102.6.4 24%

```
Nov 28, 2019 @ 00:51:20.000  @timestamp: Nov 28, 2019 @ 00:51:20.000 event.start: Nov 28, 2019 @ 00:50:31.085 event.end: Nov 28, 2019 @ 00:50:42.170 event.duration: 11,084,759,499 event.dataset: flow
                             event.kind: event event.category: network_traffic event.action: network_flow type: flow ecs.version: 1.1.0 agent.id: b9492a28-abce-4715-ae74-c89f7c3fb0ed
                             agent.version: 7.4.2 agent.name: globo-packetbeat agent.type: packetbeat agent.ephemeral_id: 2e34341f-7a41-4774-bf85-33020739e82a agent.hostname: globomantics-local
```

Next we can look at the destination.ip and see who the top value is.



Top 5 values in 358 / 358 records

10.102.6.5 54.7%

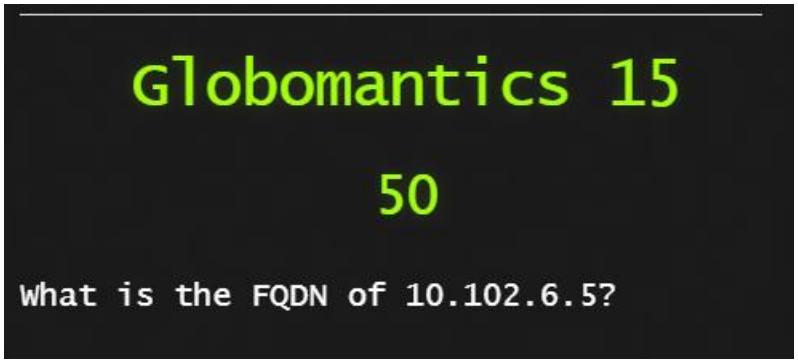
10.102.6.4 24%

10.102.3.4 6.1%

10.102.5.186 5%

10.102.5.2 4.2%

Flag: 10.102.6.5

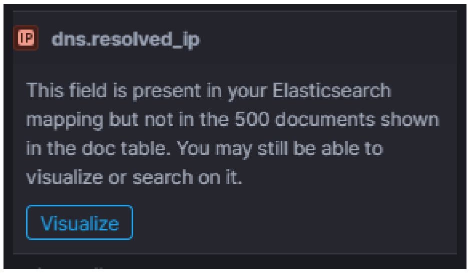


Globomantics 15

50

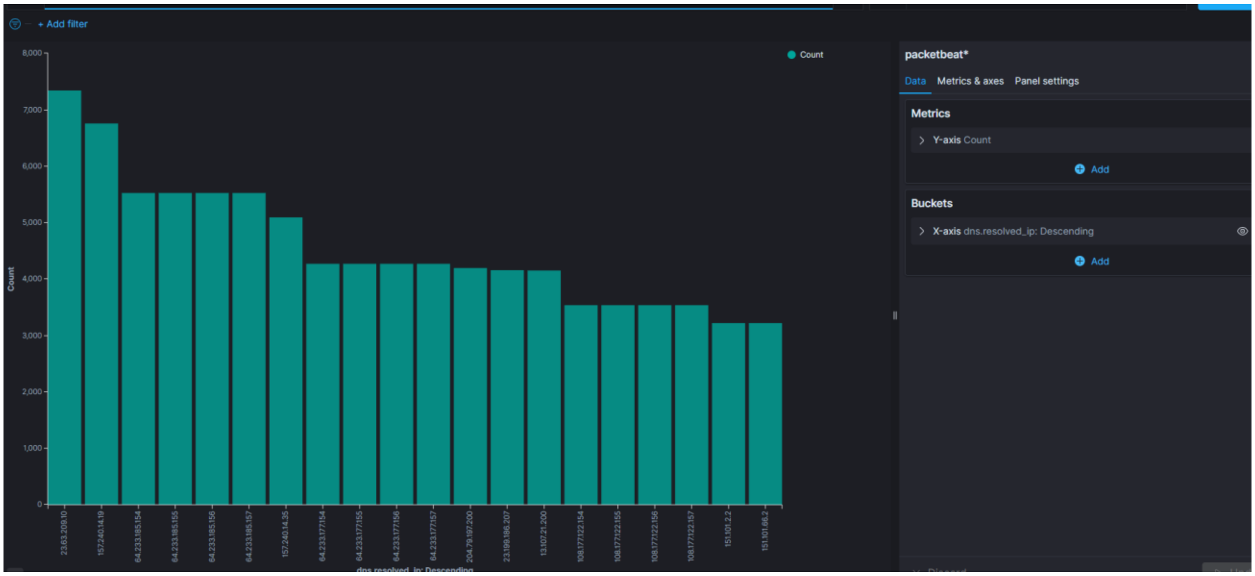
What is the FQDN of 10.102.6.5?

In packetbeat we want to look at the dns queries and in this case the dns.resolved_ip since there are over 15m packets the visual will be empty, but we will click on visualize it.



IP dns.resolved_ip

This field is present in your Elasticsearch mapping but not in the 500 documents shown in the doc table. You may still be able to visualize or search on it.

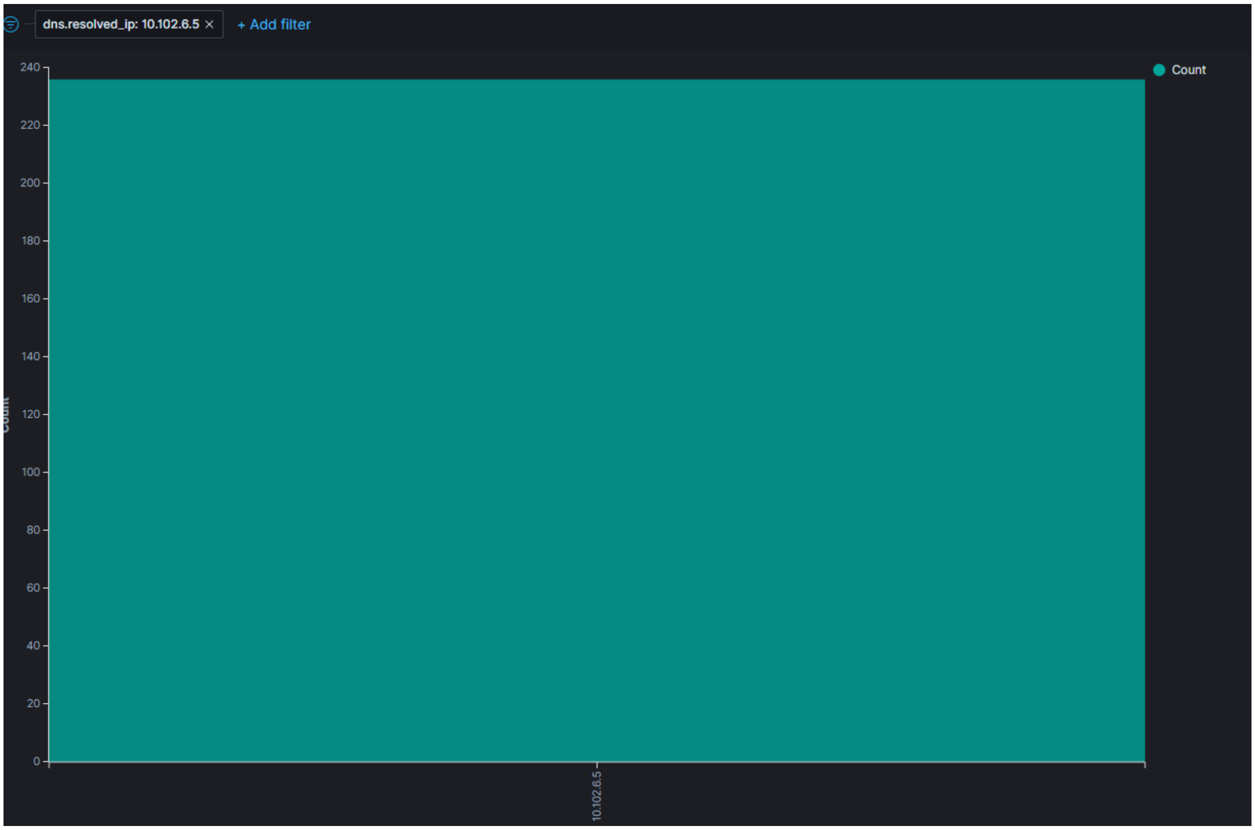


packetbeat*

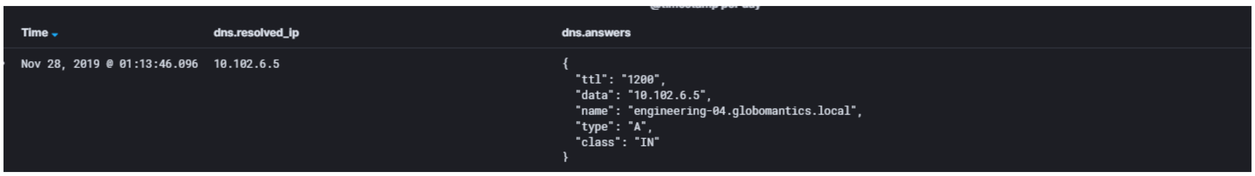
Metrics: Y-axis Count

Buckets: X-axis dns.resolved_ip: Descending

Click on one of the ip addresses and edit the filter to out IP address and when we confirm that we have some data there then pin and pivot to discovery.



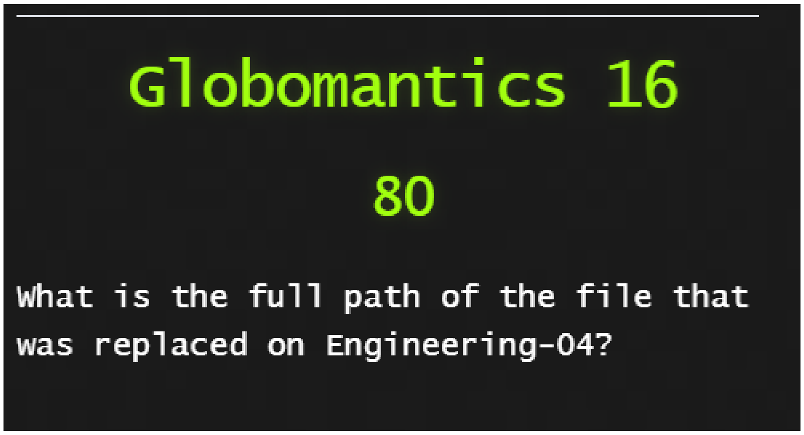
We can look at the document and see the dns.answers has what we are looking for.



Time	dns.resolved_ip	dns.answers

Nov 28, 2019 @ 01:13:46.096	10.102.6.5	{
		"ttl": "1200",
		"data": "10.102.6.5",
		"name": "engineering-04.globomantics.local",
		"type": "A",
		"class": "IN"
		}

Flag: engineering-04.globomantics.local



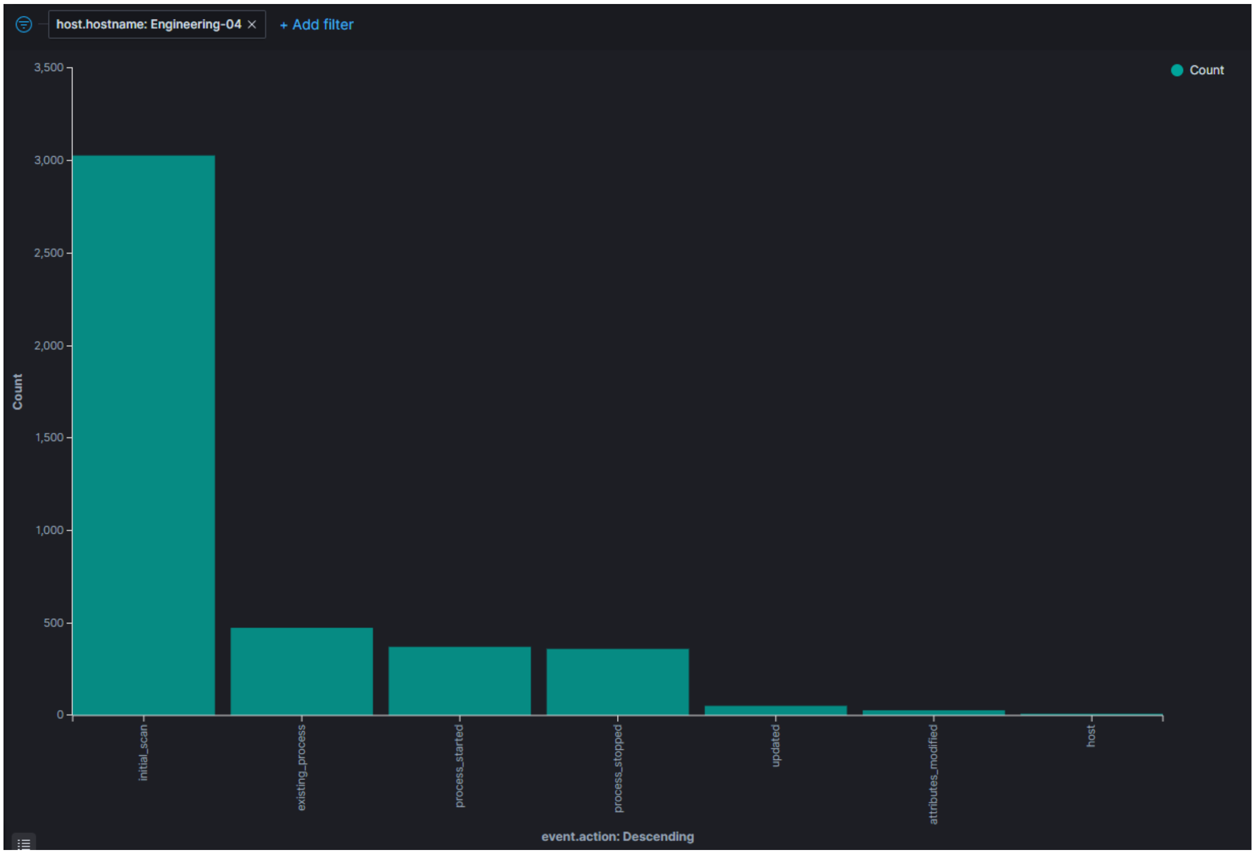
Globomantics 16

80

What is the full path of the file that was replaced on Engineering-04?

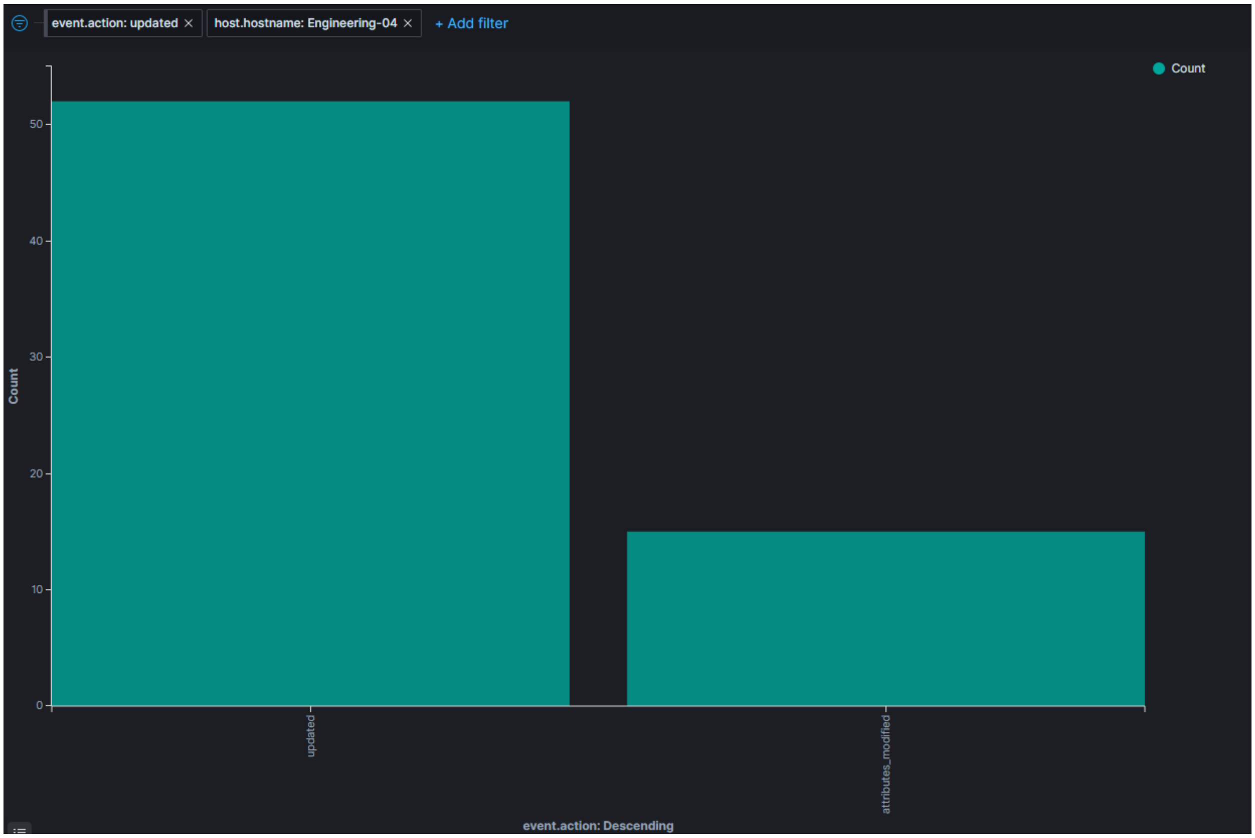
We need to look back at the auditbeat data and we need to select the host.hostname: Engineering-4

And we want to look at the event.action in a visual to see what type of events we can look closer at.

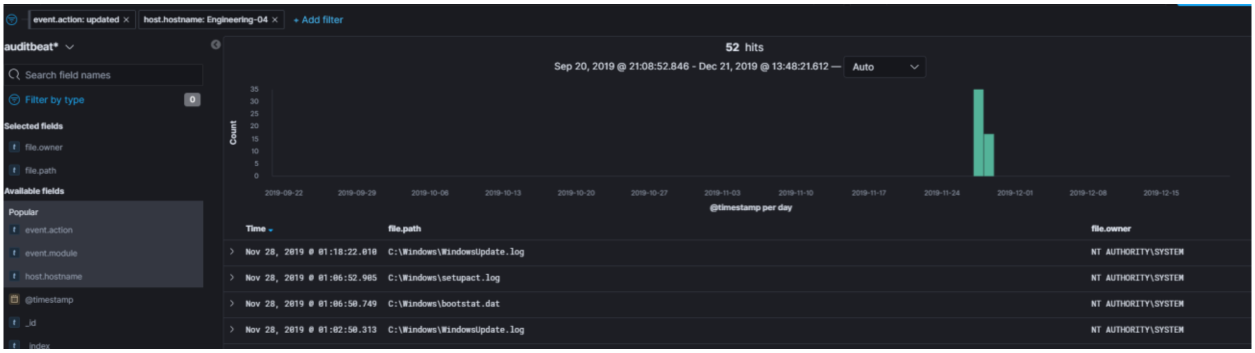


host.hostname: Engineering-04

When a file gets replaced it might be considered updated. So, we will pivot to that event.action.



I pinned them items to the bar and moved over to the discovery tab and added file.owner and file.path to the display to make it easier to see what we are looking at.



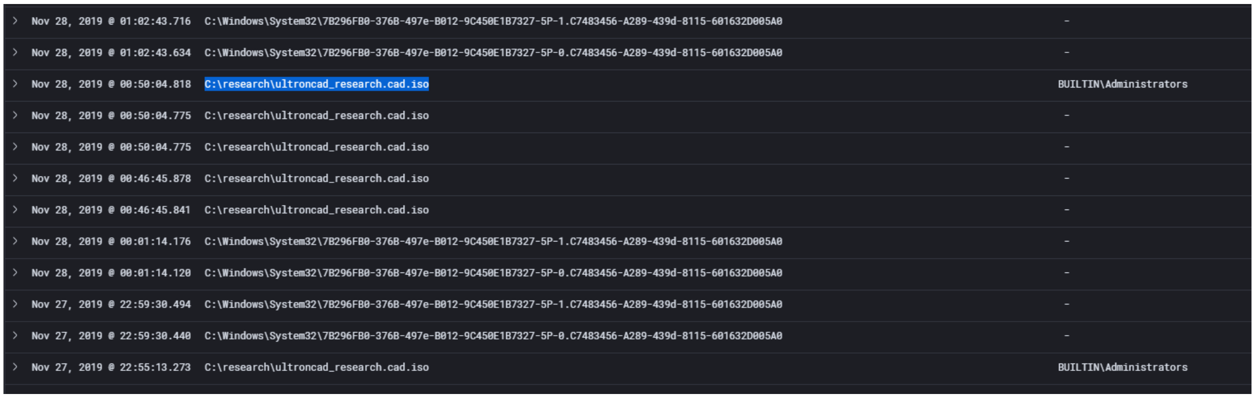
52 hits

Sep 20, 2019 @ 21:08:52.846 - Dec 21, 2019 @ 13:48:21.612 —

Time	file.path	file.owner
Nov 28, 2019 @ 01:18:22.010	C:\Windows\WindowsUpdate.log	NT AUTHORITY\SYSTEM
Nov 28, 2019 @ 01:06:52.985	C:\Windows\setupact.log	NT AUTHORITY\SYSTEM
Nov 28, 2019 @ 01:06:50.749	C:\Windows\bootstat.dat	NT AUTHORITY\SYSTEM
Nov 28, 2019 @ 01:02:50.313	C:\Windows\WindowsUpdate.log	NT AUTHORITY\SYSTEM

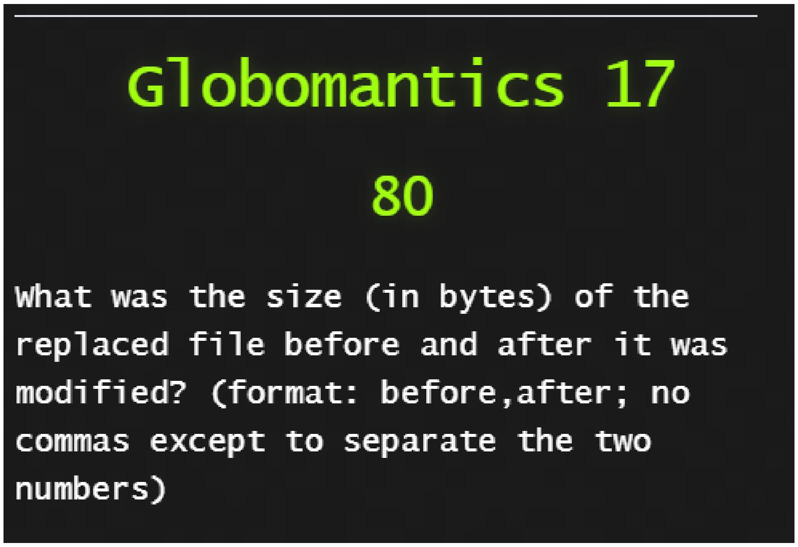
We are not interested in the stuff modified by the system so we can hide NT Authority

All we have left is a file modified by a builtin\Administrator



```
Nov 28, 2019 @ 01:02:43.716  C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0   -
Nov 28, 2019 @ 01:02:43.634  C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0   -
Nov 28, 2019 @ 00:50:04.818  C:\research\ultroncad_research.cad.iso                                                                BUILTIN\Administrators
Nov 28, 2019 @ 00:50:04.775  C:\research\ultroncad_research.cad.iso                                                                 -
Nov 28, 2019 @ 00:50:04.775  C:\research\ultroncad_research.cad.iso                                                                 -
Nov 28, 2019 @ 00:46:45.878  C:\research\ultroncad_research.cad.iso                                                                 -
Nov 28, 2019 @ 00:46:45.841  C:\research\ultroncad_research.cad.iso                                                                 -
Nov 28, 2019 @ 00:01:14.176  C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0   -
Nov 28, 2019 @ 00:01:14.120  C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0   -
Nov 27, 2019 @ 22:59:30.494  C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0   -
Nov 27, 2019 @ 22:59:30.440  C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0   -
Nov 27, 2019 @ 22:55:13.273  C:\research\ultroncad_research.cad.iso                                                                BUILTIN\Administrators
```

Flag: C:\research\ultroncad_research.cad.iso

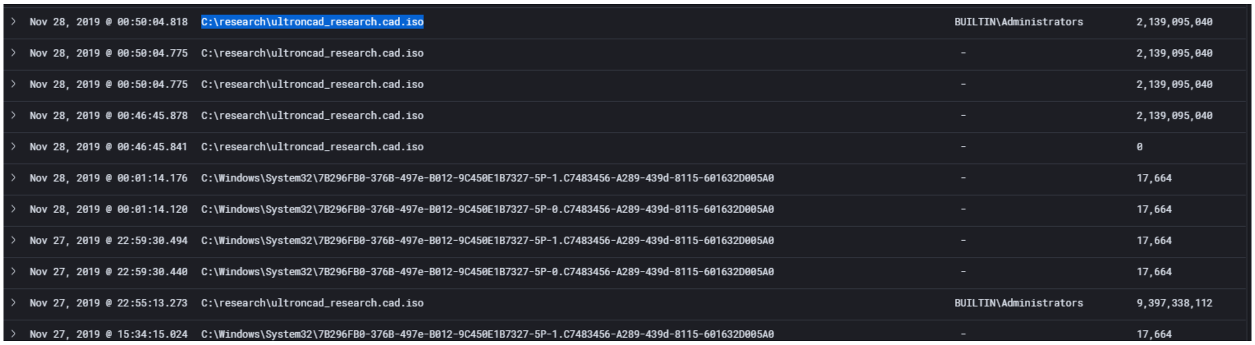


Globomantics 17

80

What was the size (in bytes) of the replaced file before and after it was modified? (format: before,after; no commas except to separate the two numbers)

For this we just need to add the column file.size to see that two different sizes.



Nov 28, 2019 @ 00:50:04.818	C:\research\ultroncad_research.cad.iso	BUILTIN\Administrators	2,139,095,040
Nov 28, 2019 @ 00:50:04.775	C:\research\ultroncad_research.cad.iso	-	2,139,095,040
Nov 28, 2019 @ 00:50:04.775	C:\research\ultroncad_research.cad.iso	-	2,139,095,040
Nov 28, 2019 @ 00:46:45.878	C:\research\ultroncad_research.cad.iso	-	2,139,095,040
Nov 28, 2019 @ 00:46:45.841	C:\research\ultroncad_research.cad.iso	-	0
Nov 28, 2019 @ 00:01:14.176	C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0	-	17,664
Nov 28, 2019 @ 00:01:14.120	C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0	-	17,664
Nov 27, 2019 @ 22:59:30.494	C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0	-	17,664
Nov 27, 2019 @ 22:59:30.440	C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0	-	17,664
Nov 27, 2019 @ 22:55:13.273	C:\research\ultroncad_research.cad.iso	BUILTIN\Administrators	9,397,338,112
Nov 27, 2019 @ 15:34:15.024	C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0	-	17,664

Flag: 9397338112,2139095040