TASK 6 - TECHNICAL APPENDIX

Rev D

Cyber Team 10

Authored by: S. Voss

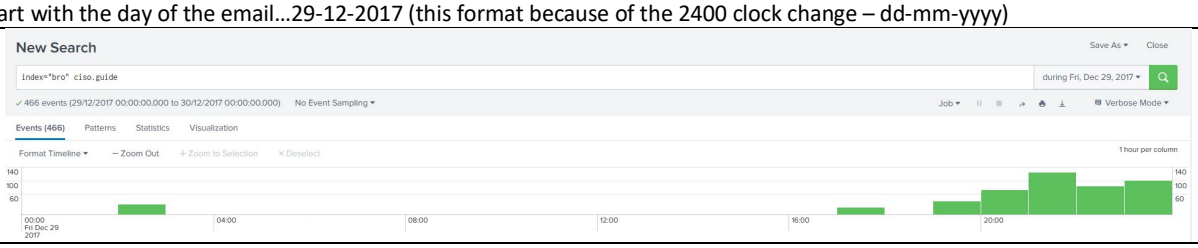
TABLE OF CONTENTS

1 - SEARCH AND DISCOVERY

Option to set the time format to 2400
Change US to GB in address line…

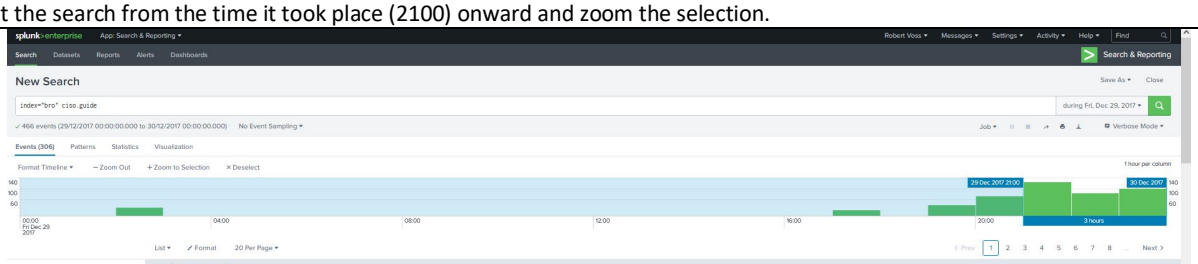
to

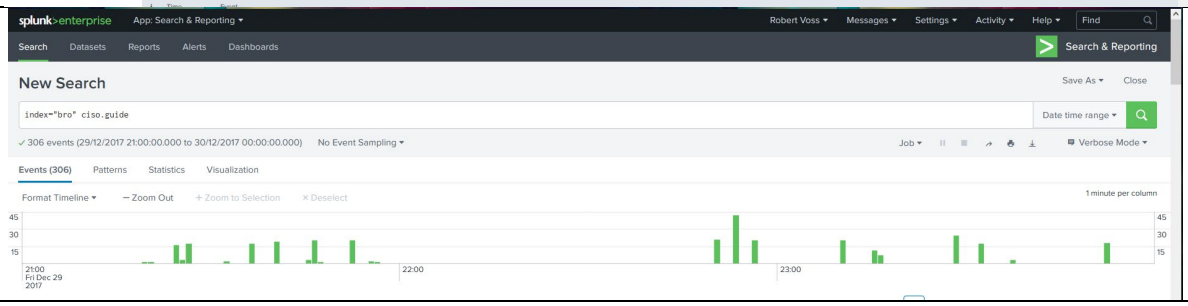

Start with the day of the email…29-12-2017 (this format because of the 2400 clock change – dd-mm-yyyy)



The email arrived at 15:58 EST (converted to UCT makes it 20:58)

Set the search from the time it took place (2100) onward and zoom the selection.





Analyzing the suspicious email shows it aimed to convince recipients to visit ciso[.]guide.
The exploration led us to consider the possibility of a drive-by compromise as an initial access method. Simply browsing a compromised site could introduce malware to a system.
With this knowledge, we dove into our SIEM logs, focusing on network traffic connected to ciso[.]guide—the potentially compromised site.
While navigating the logs, we came across the http_referrer field, a useful indicator of origin and redirection in web traffic.

We then asked, where was traffic from ciso[.]guide being referred to?

Our search for traffic originating from ciso[.]guide but being referred elsewhere unveiled anomalies: unresolved domain names and excessively complex URIs.

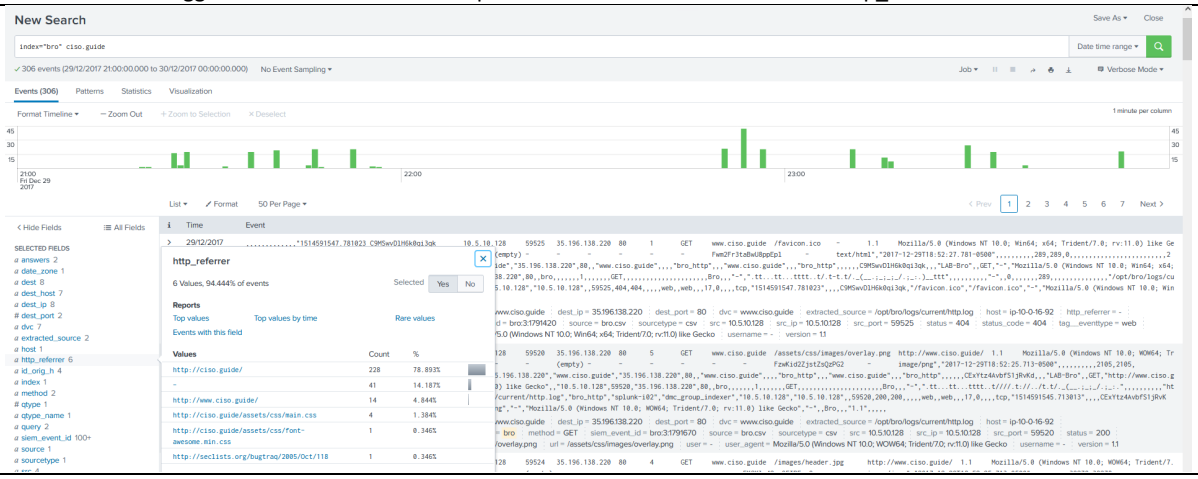
Digging deeper, we pinpointed the IP address associated with these anomalies and conducted further investigations online. Our findings confirmed our suspicions: the logs indicated encounters with a Rig EK landing page by four AT-USA devices.

When we first got into the SIEM, we had no idea what kind of information would be contained in each of the available log sources. We had to profile each log source, which meant manually exploring each index and literally just start clicking on stuff. There was no other way to go about it. As we were going through this process, we stumbled upon the http_referrer field.

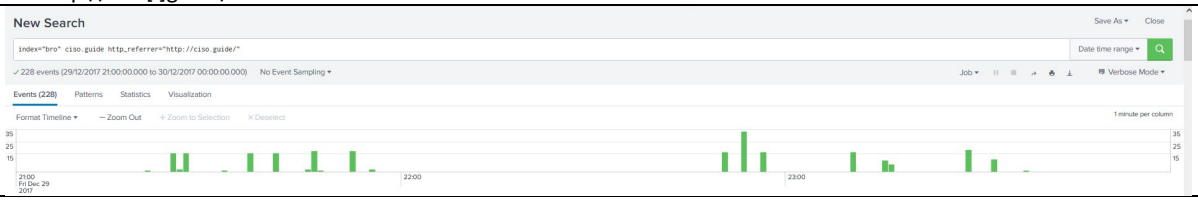
Interpreting the field name:
"http" relates to web traffic.
"referrer" indicated the referral or redirection of traffic.

We selected that field and conducted some searches with it until we stumbled upon the weird stuff.

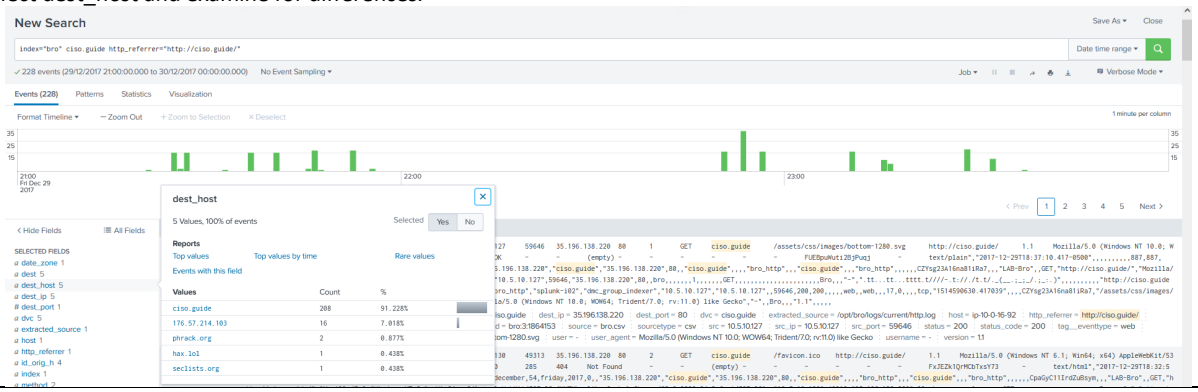
Because the email suggested to visit a website an option in the search was to select the http_referrer field.



Select http://ciso[.]guide/ which matches the link in the email



Continuing to investigate the various fields
Select dest_host and examine for differences.



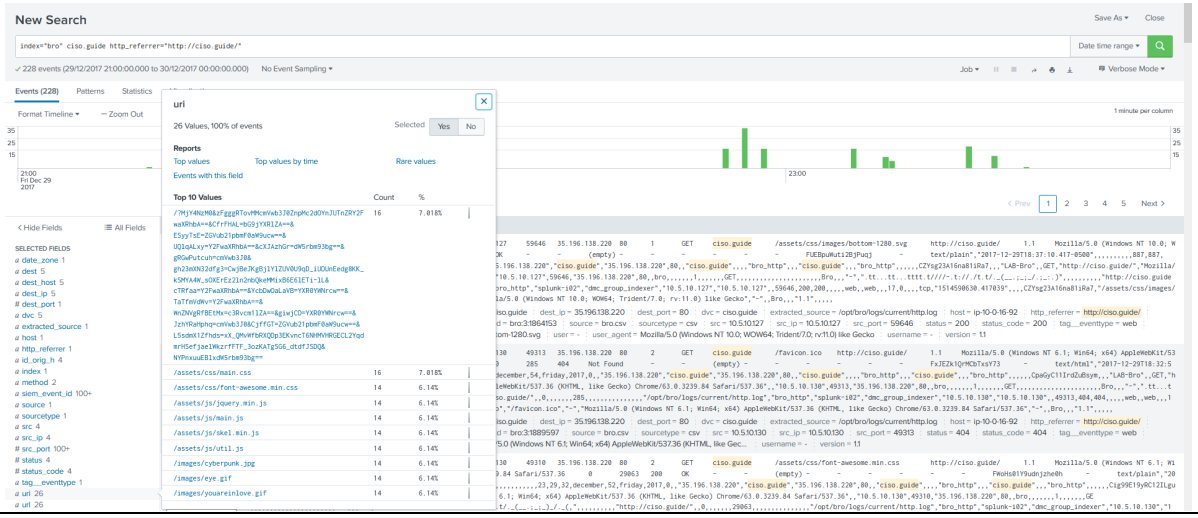
Notice one value is an ip address and not a resolved domain name.
176.57.214.103 (this is not correct and a sign of a possible problem).

Continuing to investigate the various fields
Select dest_ip and examine.

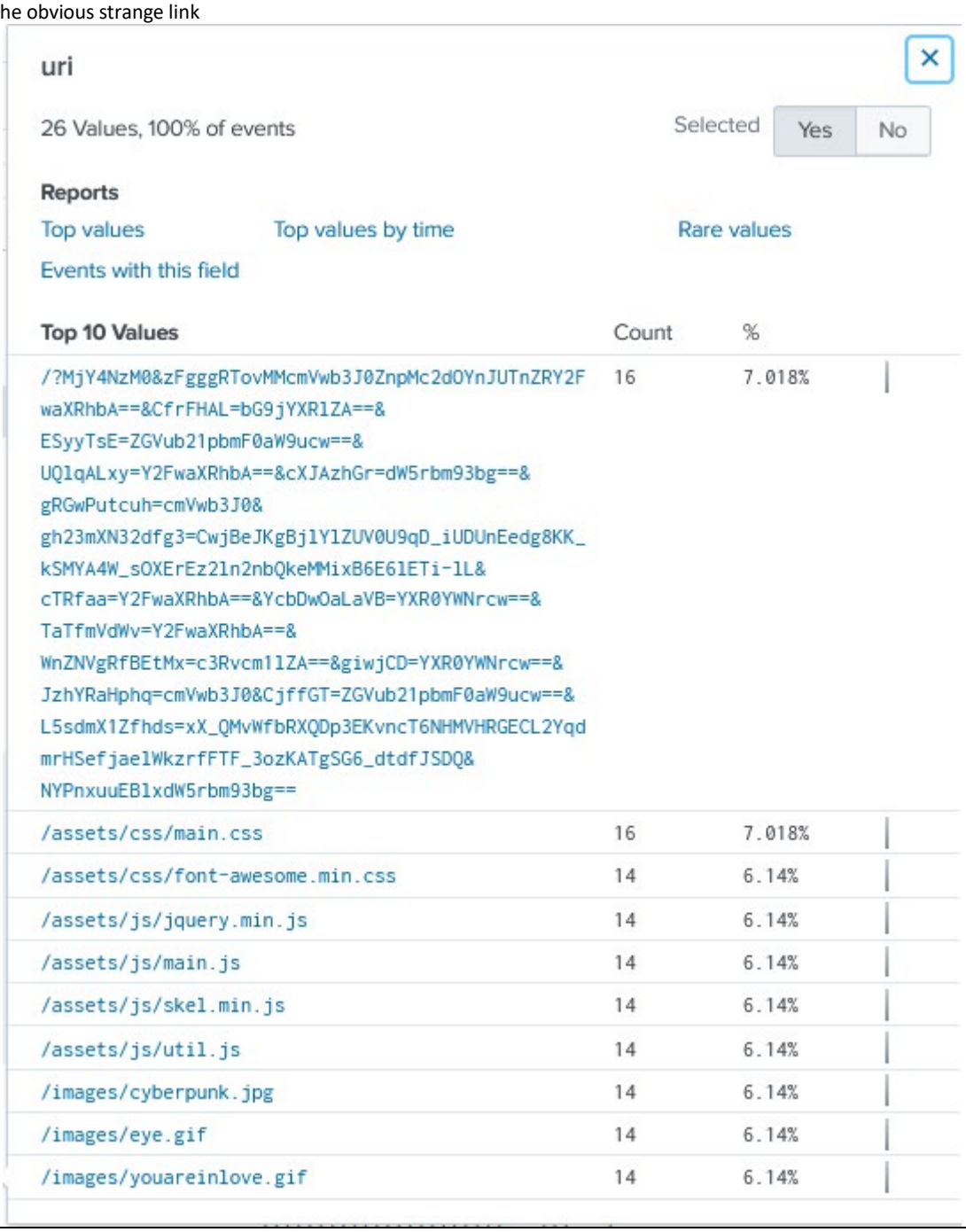
Inspect dest_ip

ip 176.57.214.103 is seen again

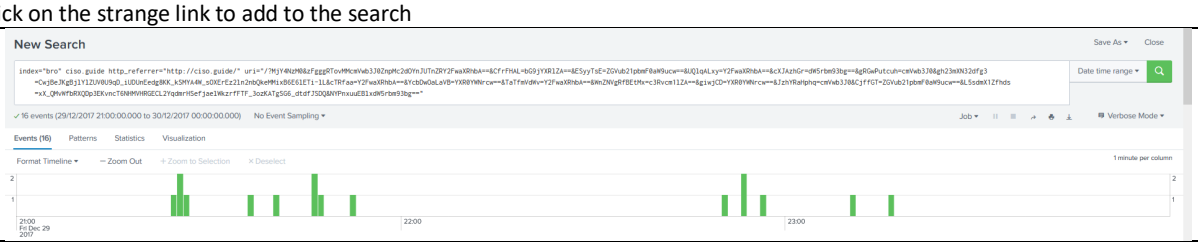
Continuing to investigate the various fields
Select uri field and examine.



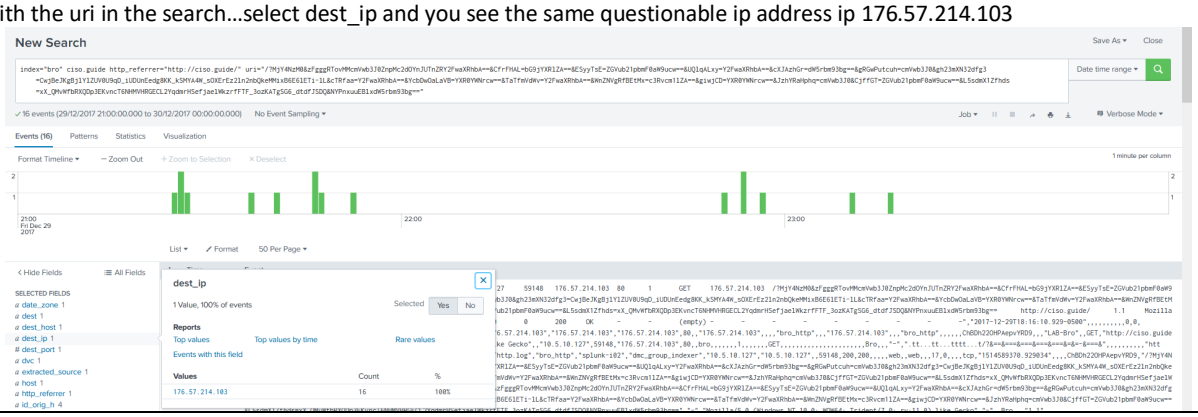
Notice the obvious strange link



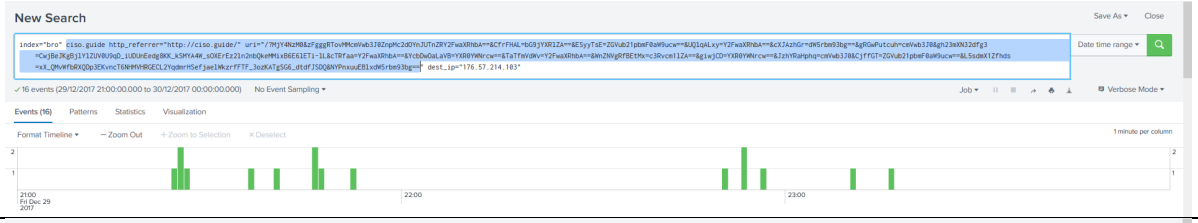
Click on the strange link to add to the search

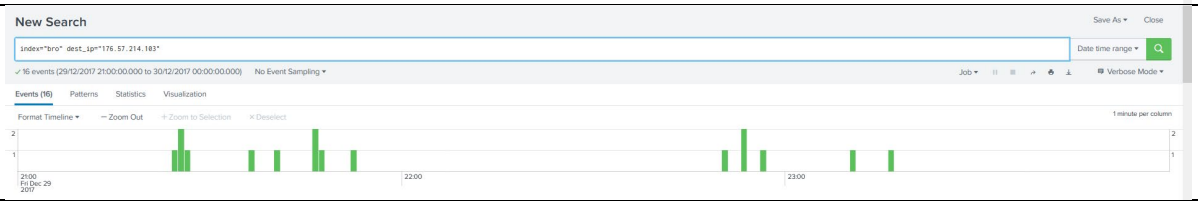


With the uri in the search…select dest_ip and you see the same questionable ip address ip 176.57.214.103

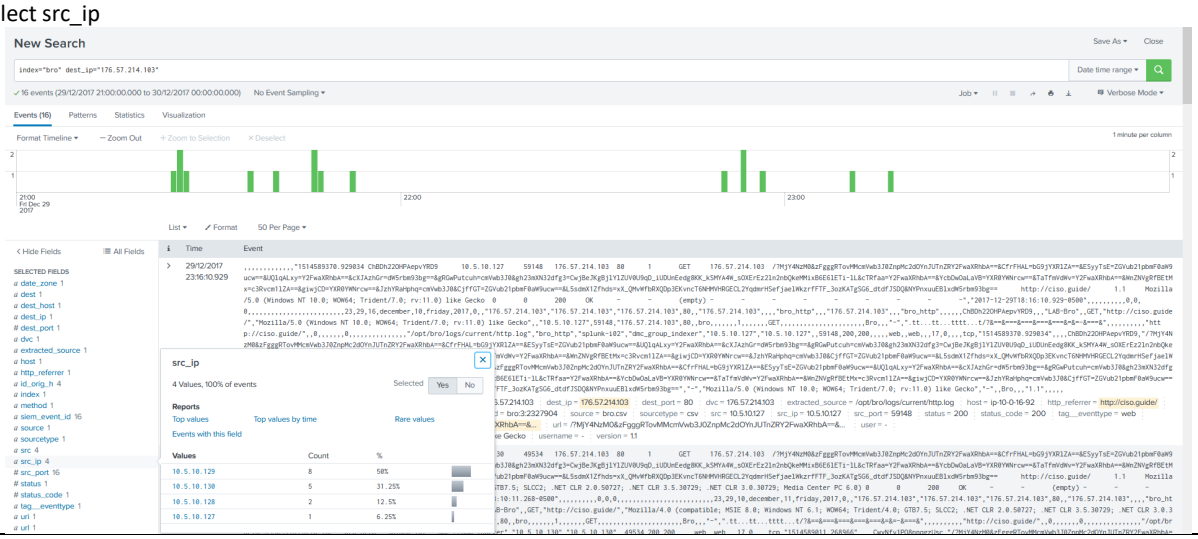


Now pivot from current search to just bro logs and the questionable ip 176.57.214.103 by clicking on the ip and trimming up the search.





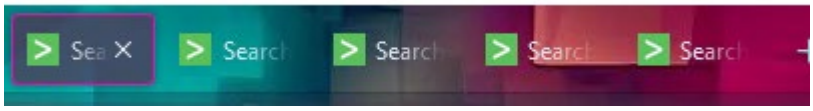
Now see who's talking to who…
Select src_ip

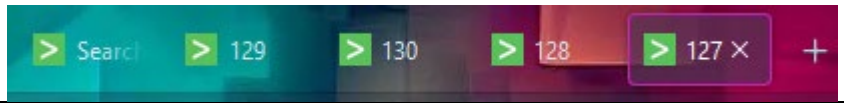


There are 4 ip addresses that are being referred over to ip 176.57.214.103

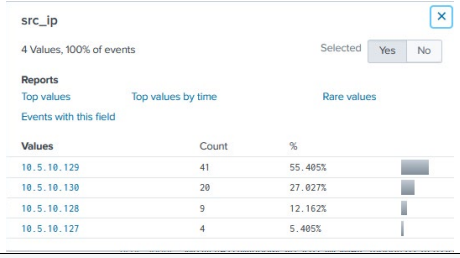
Now that the 4 devices have been identified you want to look deeper into each device…

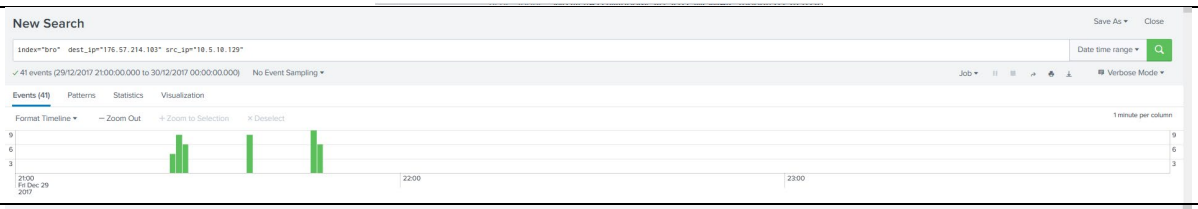
Create (duplicate) 4 tabs…one for each device and rename the tabs for ease of identification and use

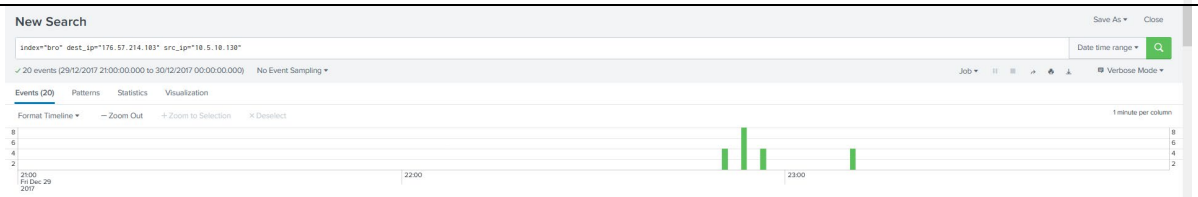


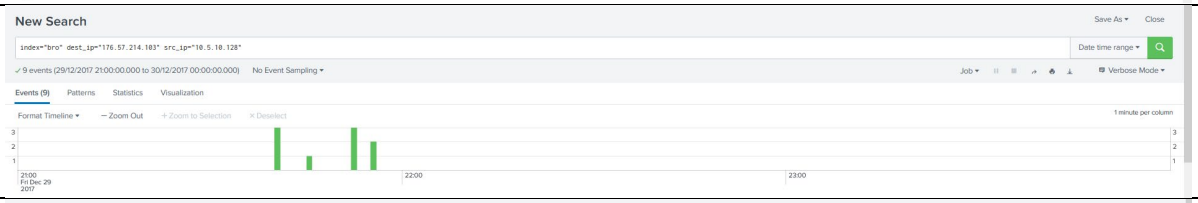


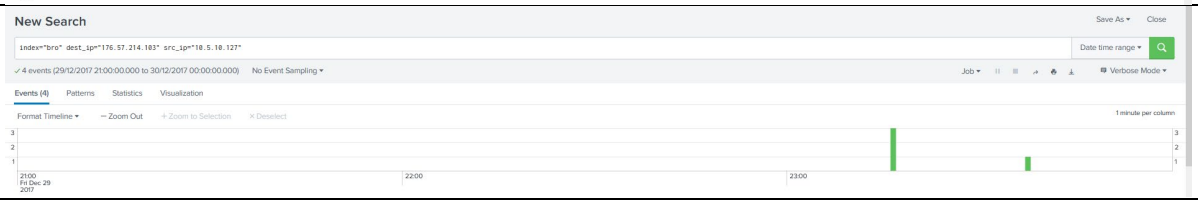
Now go into each device on each identified tab by clicking on each correlating ip address shown





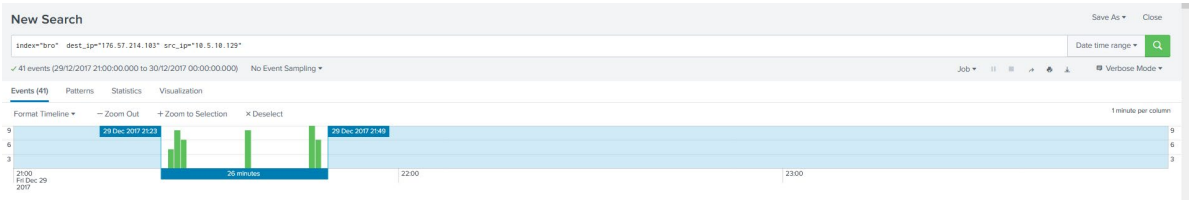




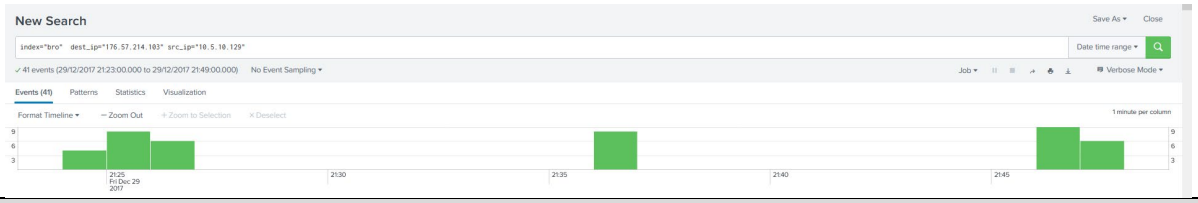


Now investigate each device separately…

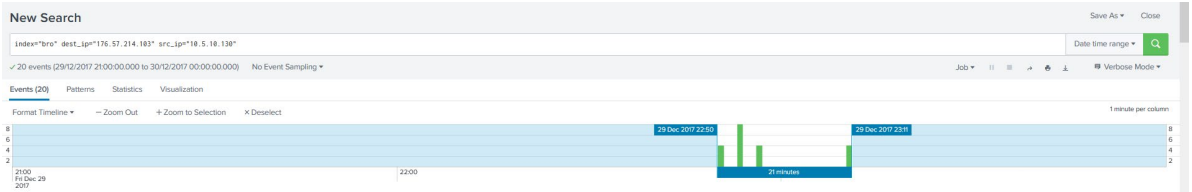
129



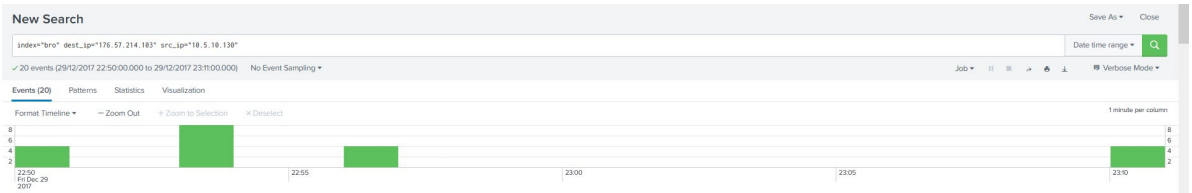
+ Zoom to selection



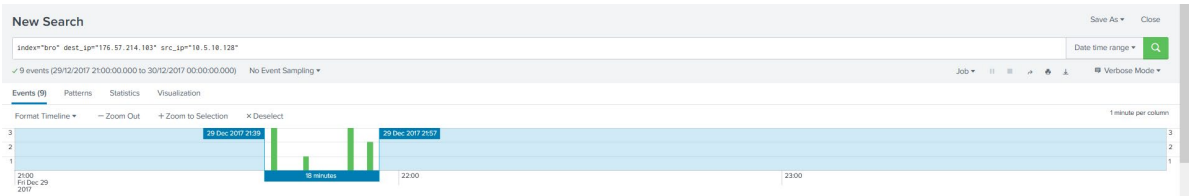
130



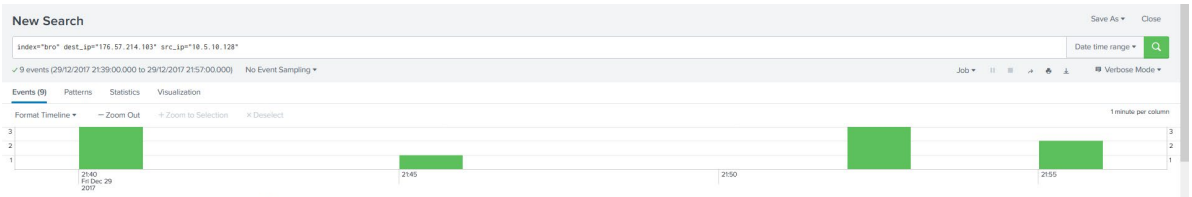
+ Zoom to selection



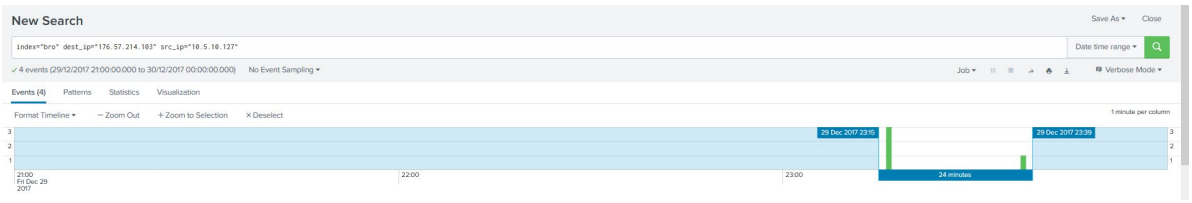
128



+ Zoom to selection

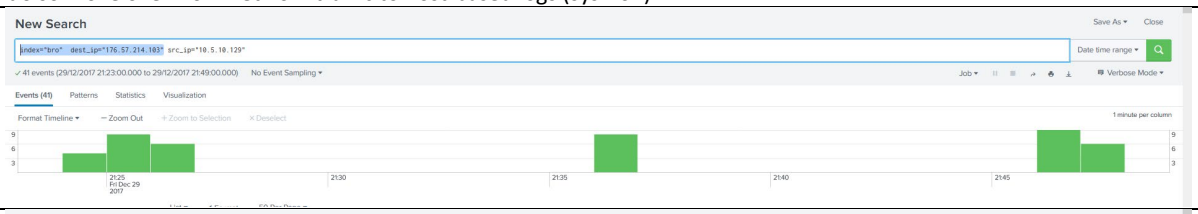


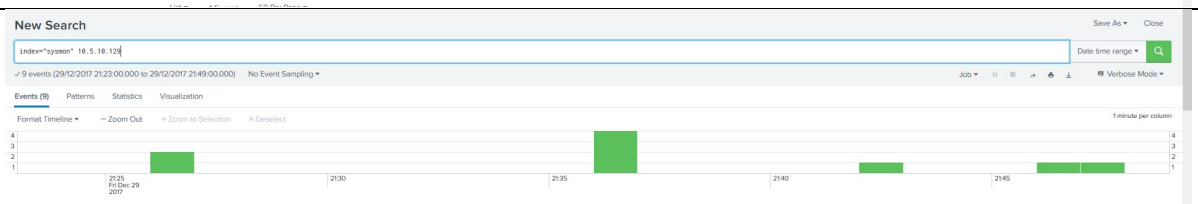
127



+ Zoom to selection

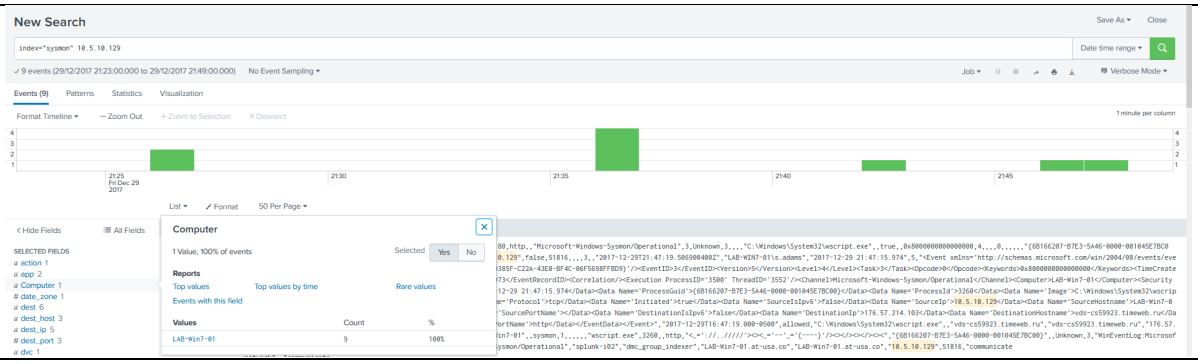
Now pivot from network traffic to host-based logs for each device by eliminating the bro from each of the searches…
To do so move over from network traffic to host-based logs (sysmon).



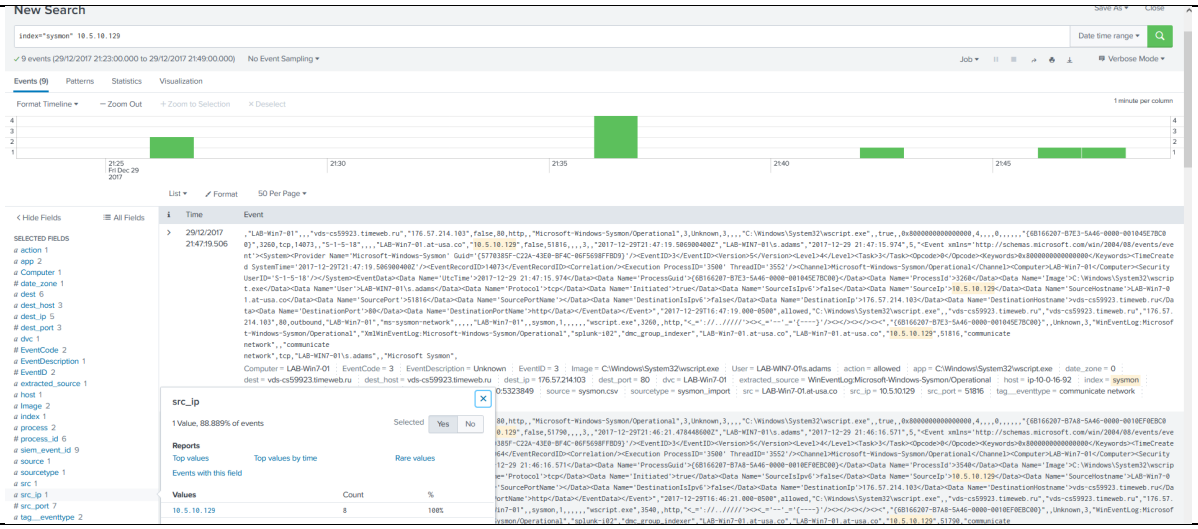


Once in host-based logs there are 9 events for 129.
Various fields to check:

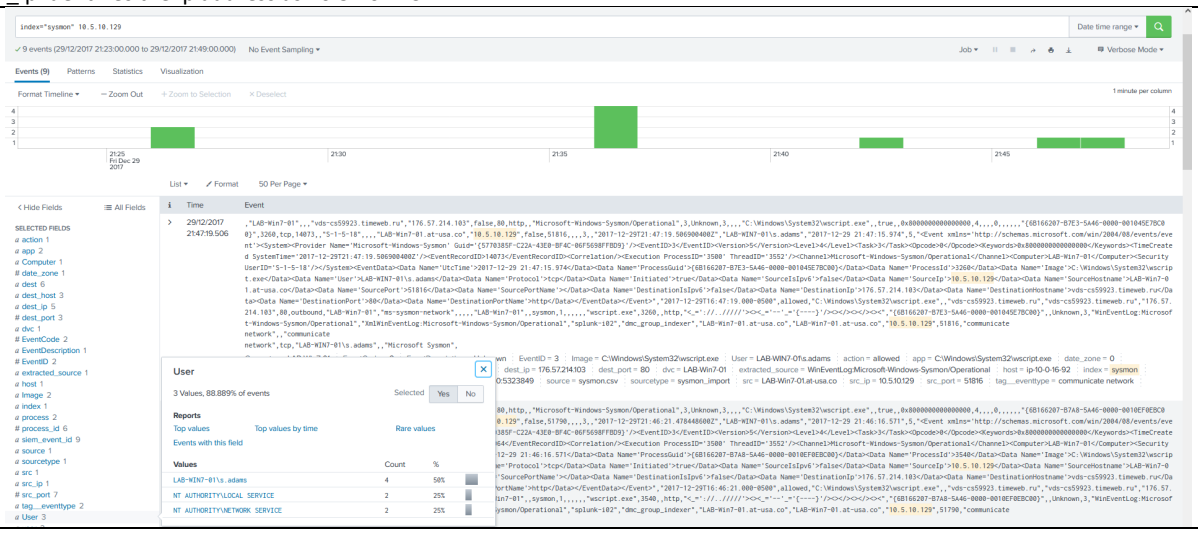
- Computer - Computer gives us the computer name which should be the main source used from now on, as ip addresses can change for each device as it logs into the network. The device name should almost ALWAYS remain the same.
- scr_ip – gives us the current operating ip address the device is using
- user – who is the user of the device



Computer gives us LAB-Win07-01 as the device name.



Scr_ip identifies the ip address as 10.5.10.129



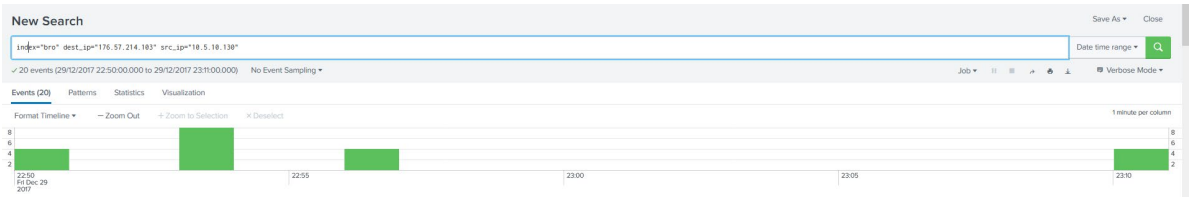
User shows LAB-Win7-01\s.adams with s.adams as the user

You can see it's
Computer: LAB-Win07-1
ip address: matches, 10.5.10.129
user: s. adams

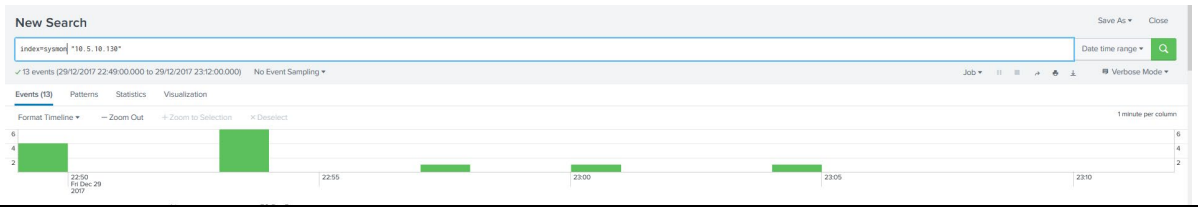
Do the same steps on all the remaining tabs

130

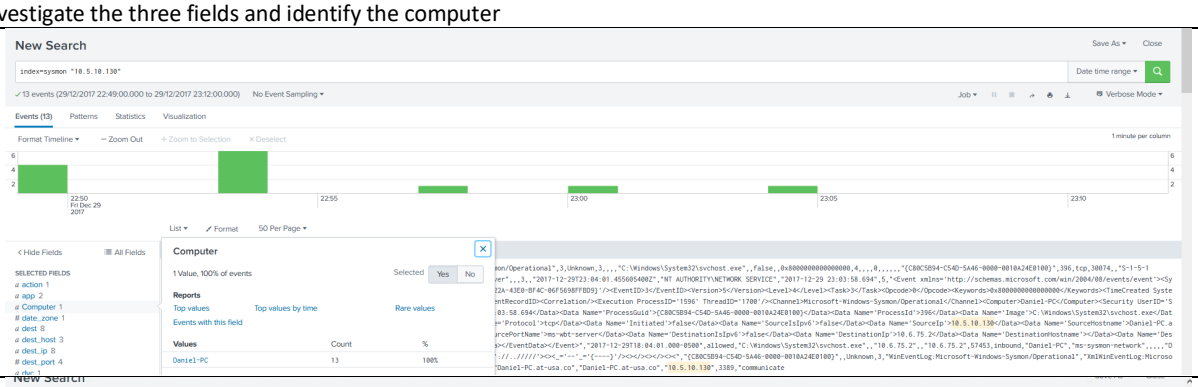
From

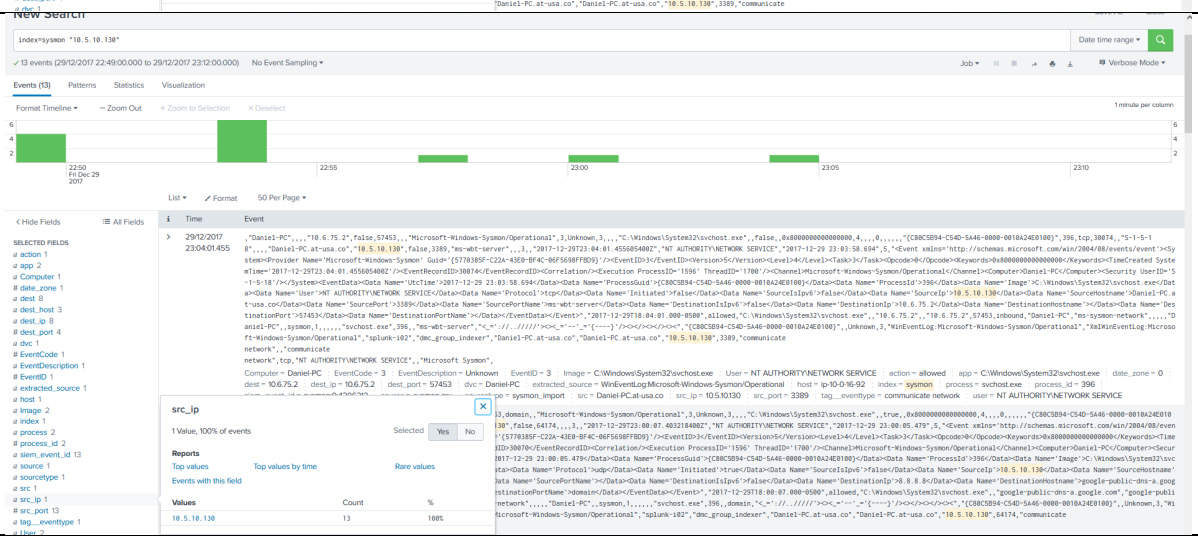


to



Investigate the three fields and identify the computer

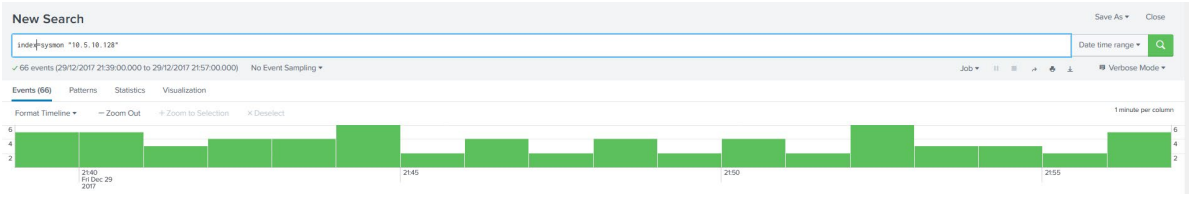




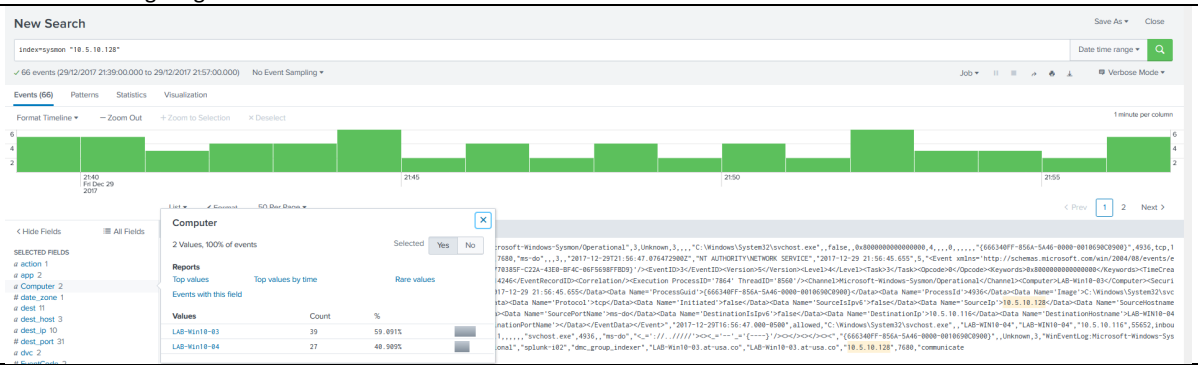
Computer: Daniel-PC
ip address: matches, 10.5.10.130
user: Daniel-PC\Daniel

128
From

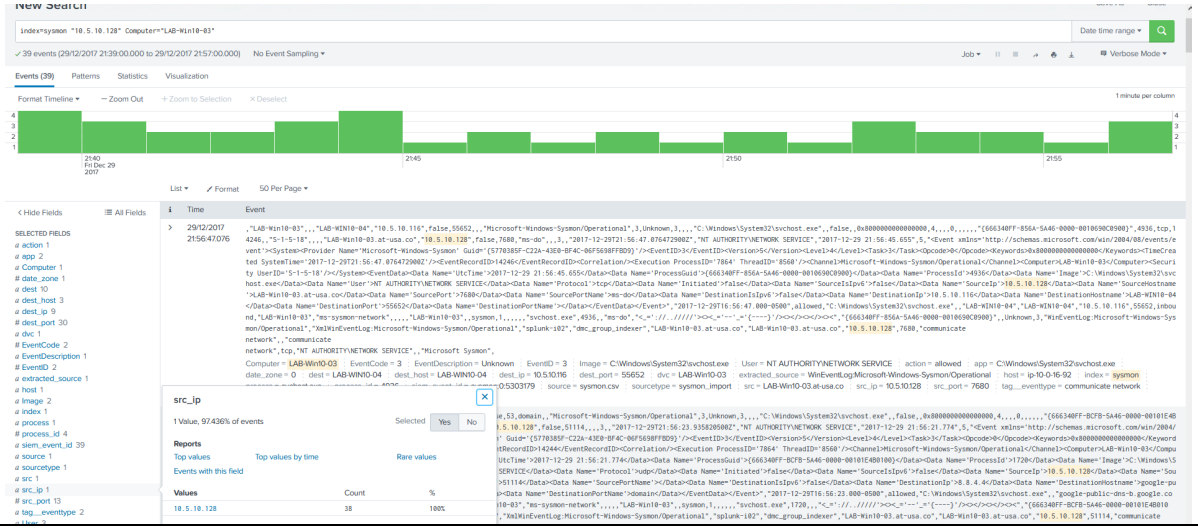
To



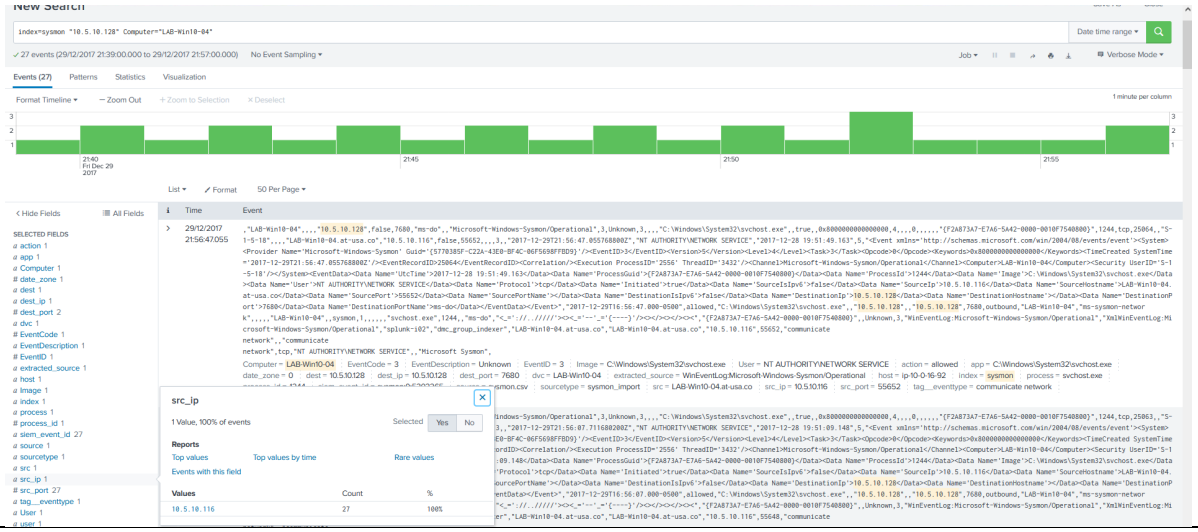
Investigate the three fields and identify the computer
Investigating 128…there are two possible computers…
Click on each computer and then select scr_ip to see which computer identifies to which and then come back and select the one we're investigating.



LAB-Win10-03

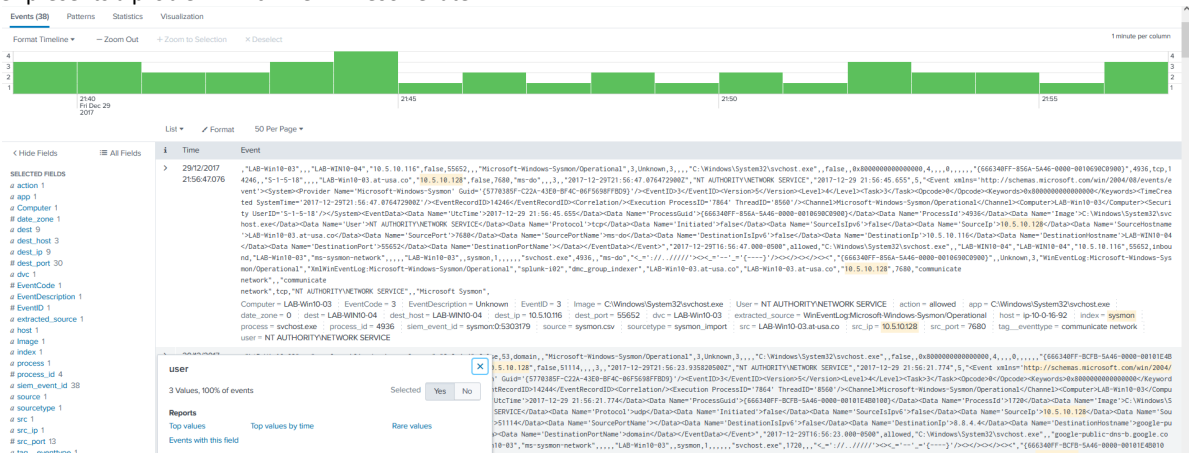


LAB-Win10-04



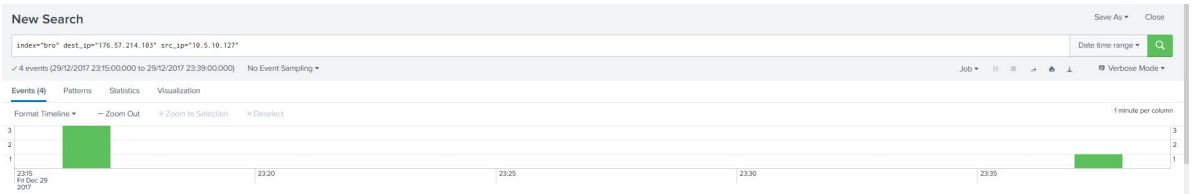
The evidence shows LAB-Win10-03 is the device name we are looking for which ties to ip 10.5.10.128.

User presents a problem which we will resolve later.

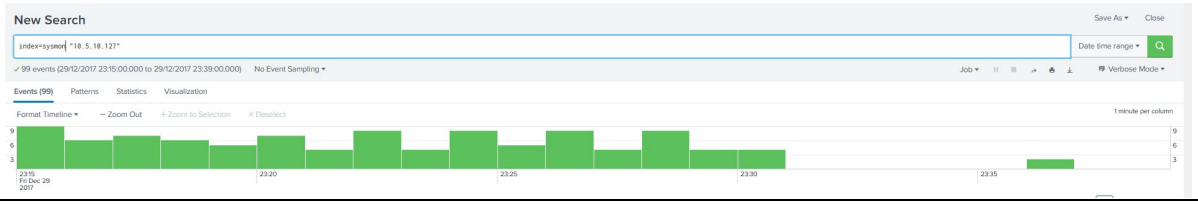


127

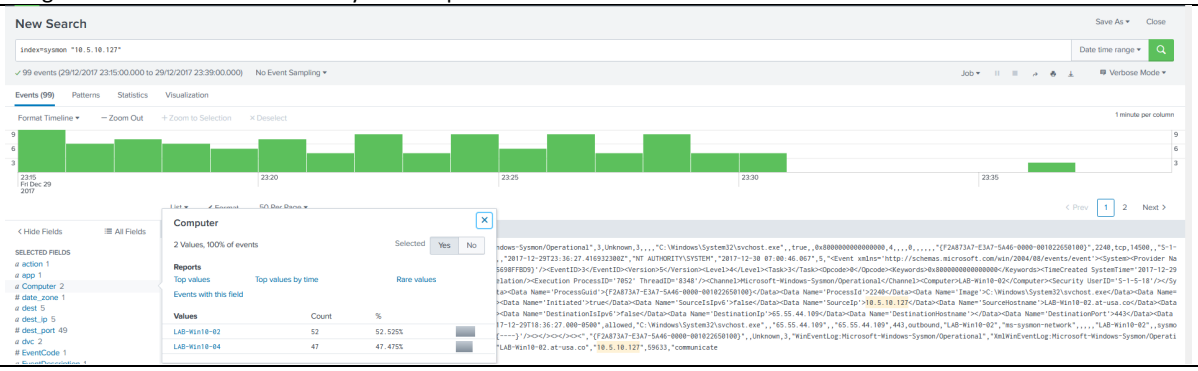
From



To

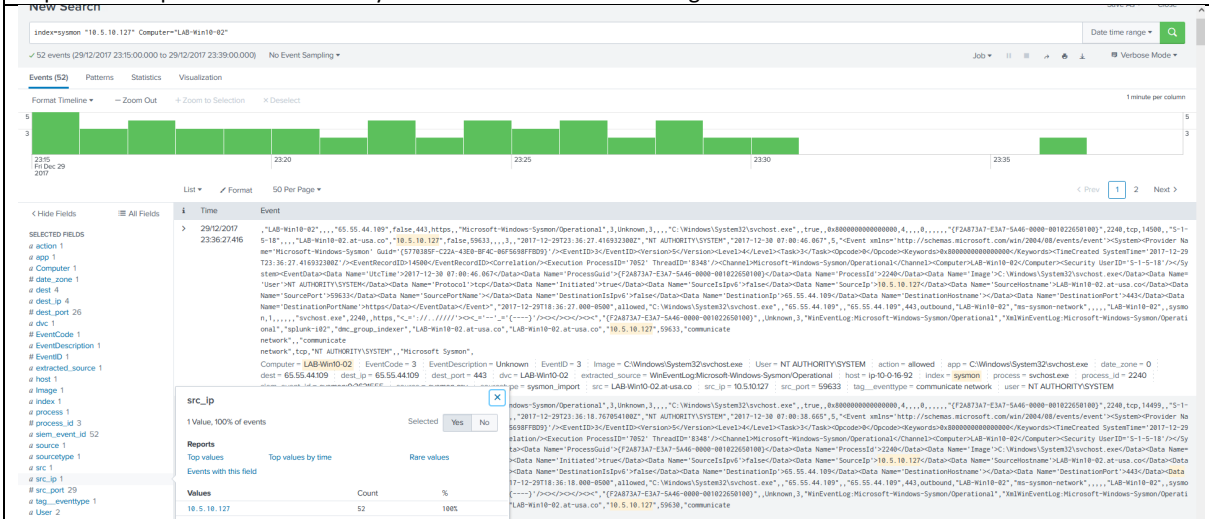


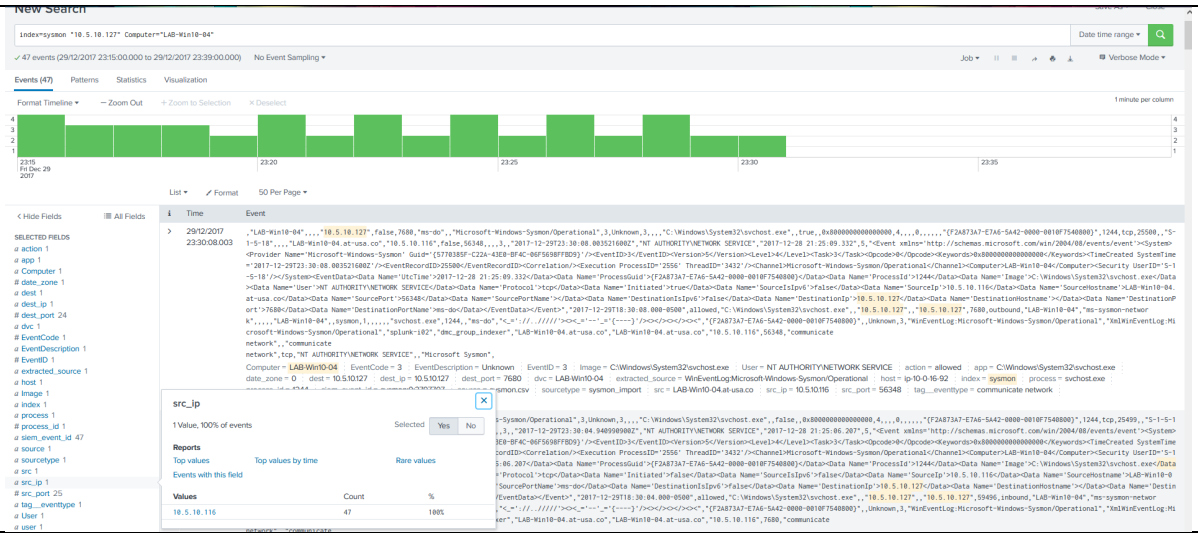
Investigate the three fields and identify the computer



As before this computer has two possibilities…

Repeat the steps as before to identify the one needed for this investigation.





The evidence shows LAB-Win10-02 is the device name we are looking for which ties to ip 10.5.10.127.

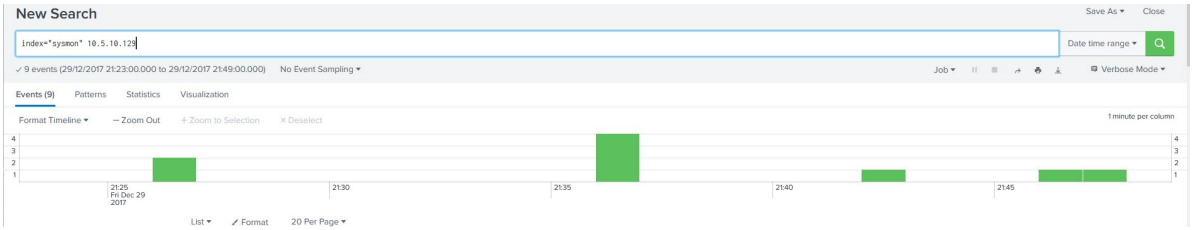
User presents a problem which we will resolve later.

With all four devices identified you need to use the computer Id and not the ip address to see all the proper Events. (This is not a network issue now but a host log search…)

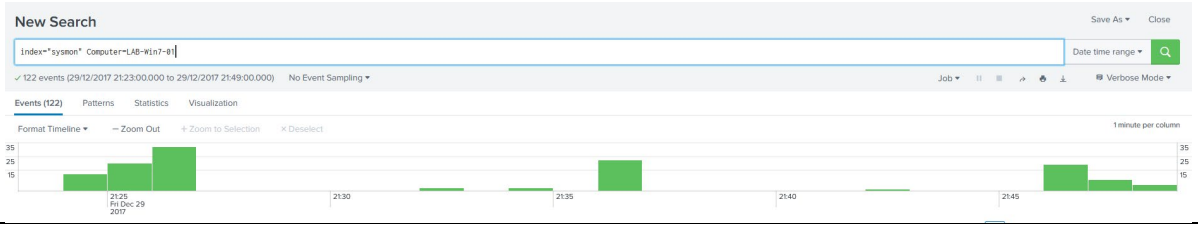
10.5.10.129 - LAB-Win7-01 - S. Adams - 8 times
10.5.10.130 - Daniel-PC – Daniel - 5 times
10.5.10.128 - LAB-Win10-03 – M. Land - 2 times
10.5.10.127 - LAB-Win10-02 – D. Walker - 1 time

Search 10.5.10.129 / LAB-Win7-01

From

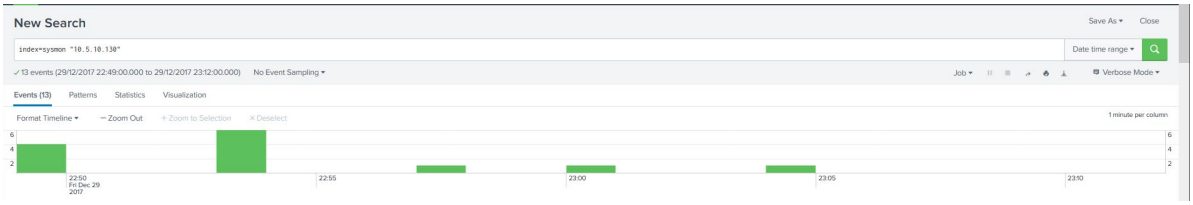


To

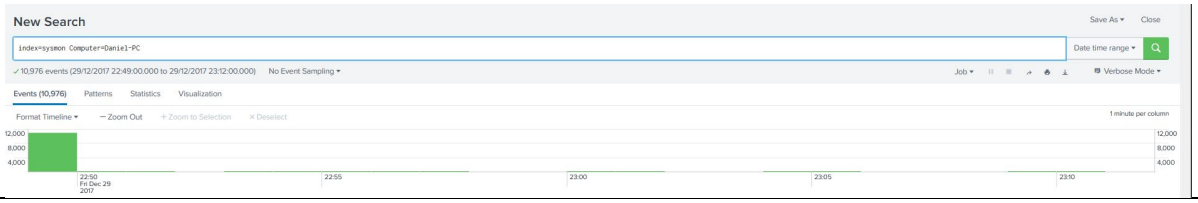


Search 10.5.10.130 / Daniel-PC

From

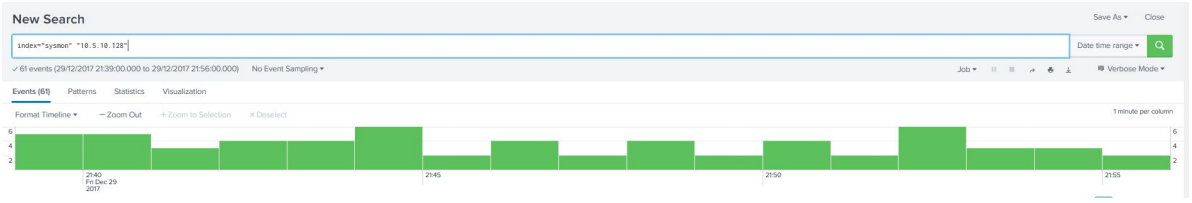


To

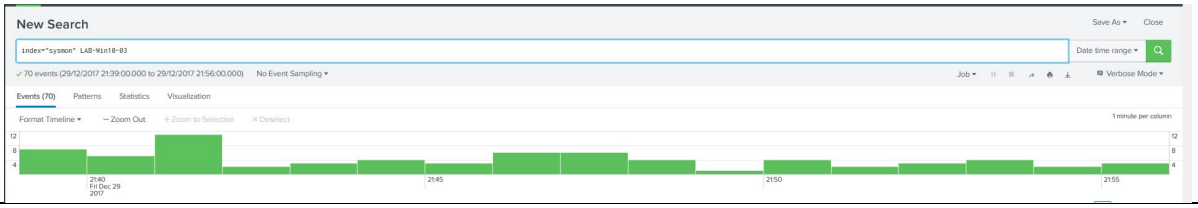


Search 10.5.10.128 / LAB-Win10-03

From

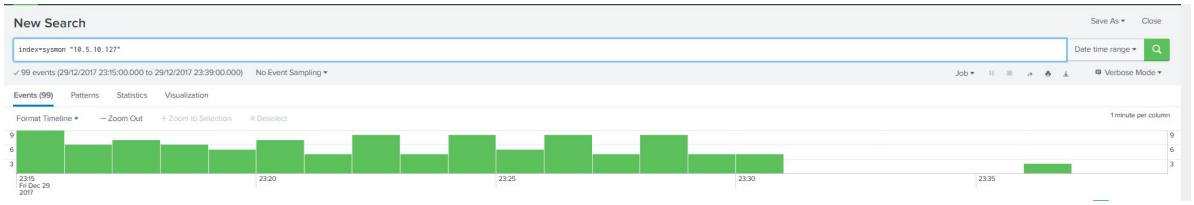


To

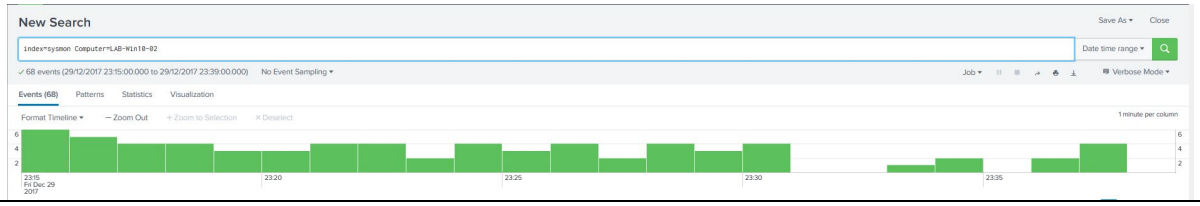


Search 10.5.10.127 / LAB-Win10-02

From

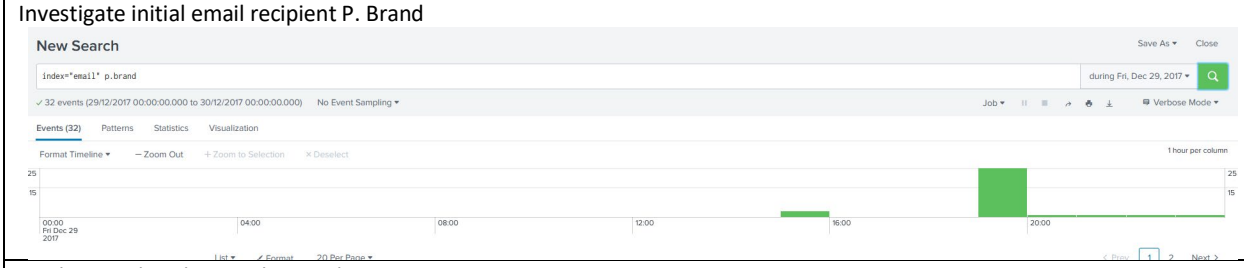


To

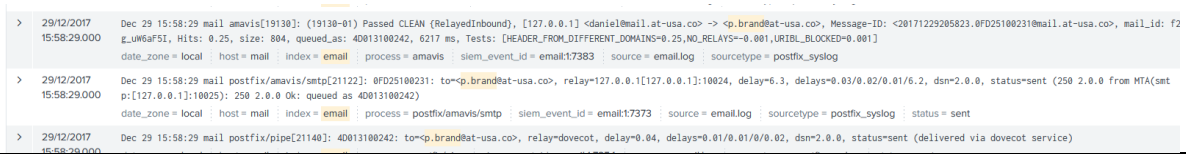


2 - IDENTIFYING EMAILS WITH TIMESTAMP

Investigate initial email recipient P. Brand

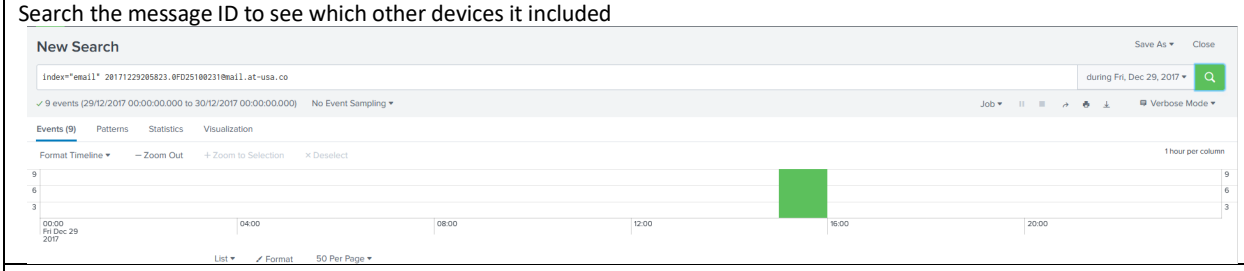


It is known that the email arrived at 15:58

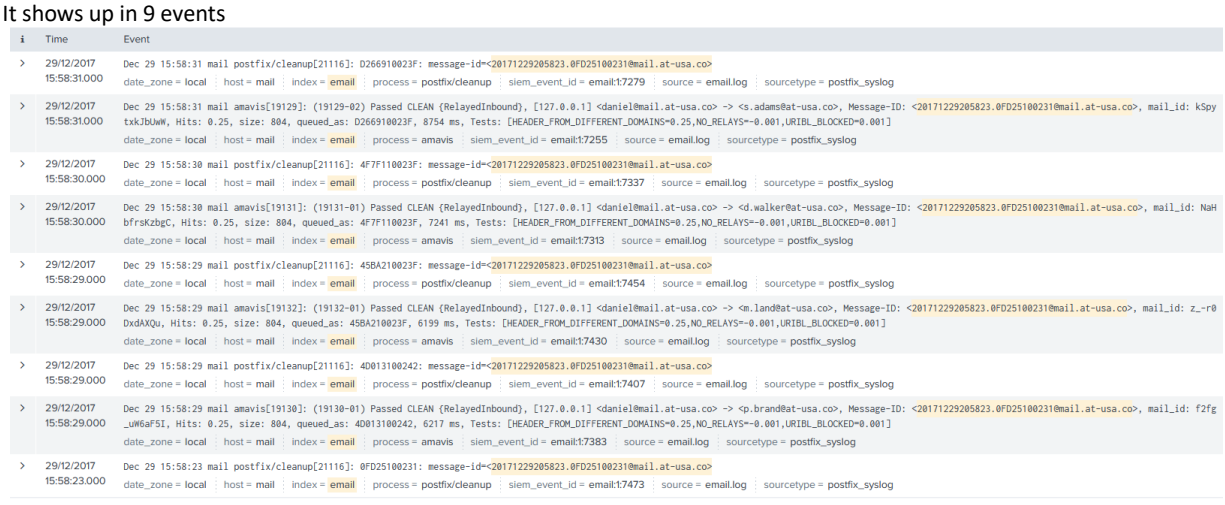


Notice the message ID

Search the message ID to see which other devices it included



It shows up in 9 events



It appears to be a spoof email from daniel@mail.at-usa.co and fired off to other colleagues.

s.adams@at-usa.co

d.walker@at-usa.co

m.land@at-usa.co

p.brand@at-usa.co

It shows there were 4 recipients…it was derived by using the message id

3 - EVENT ID 11: FILE CREATE

An EK (Exploit Kit) is to distribute Malware (delivering a payload, creating a file) on a device.
Investigate Sysmon ID's

We're looking for something that creates files

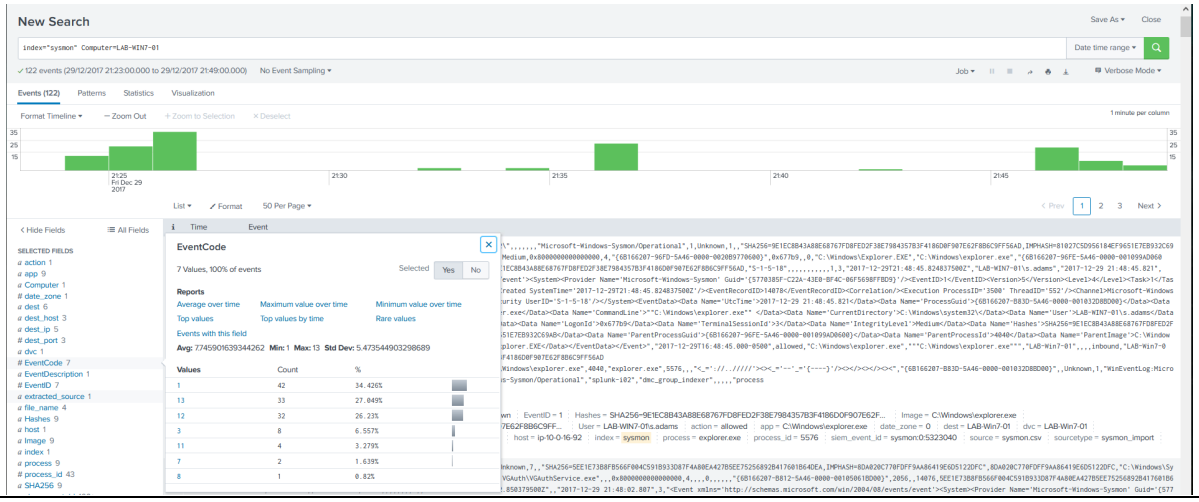
Event ID 11: FileCreate

File create operations are logged when a file is created or overwritten. This event is useful for monitoring autostart locations, like the Startup folder, as well as temporary and download directories, which are common places malware drops during initial infection.

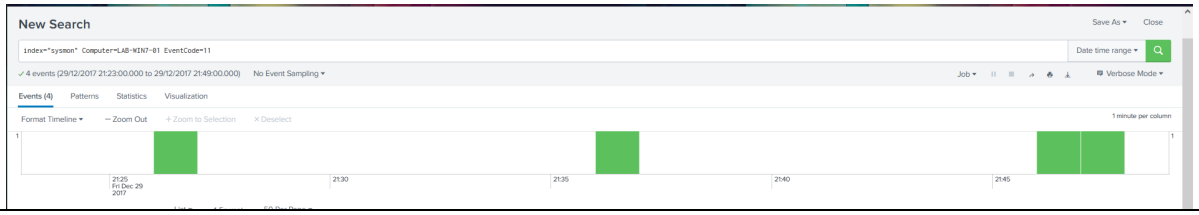
Investigate EventCode or EventID (they represent the same thing).

Select Event Code / ID 11 (File Create)
File create operations are logged when a file is created or overwritten. This event is useful for monitoring AutoStart locations, like the Startup folder, as well as temporary and download directories, which are common places malware drops during initial infection.

LAB-Win7-01



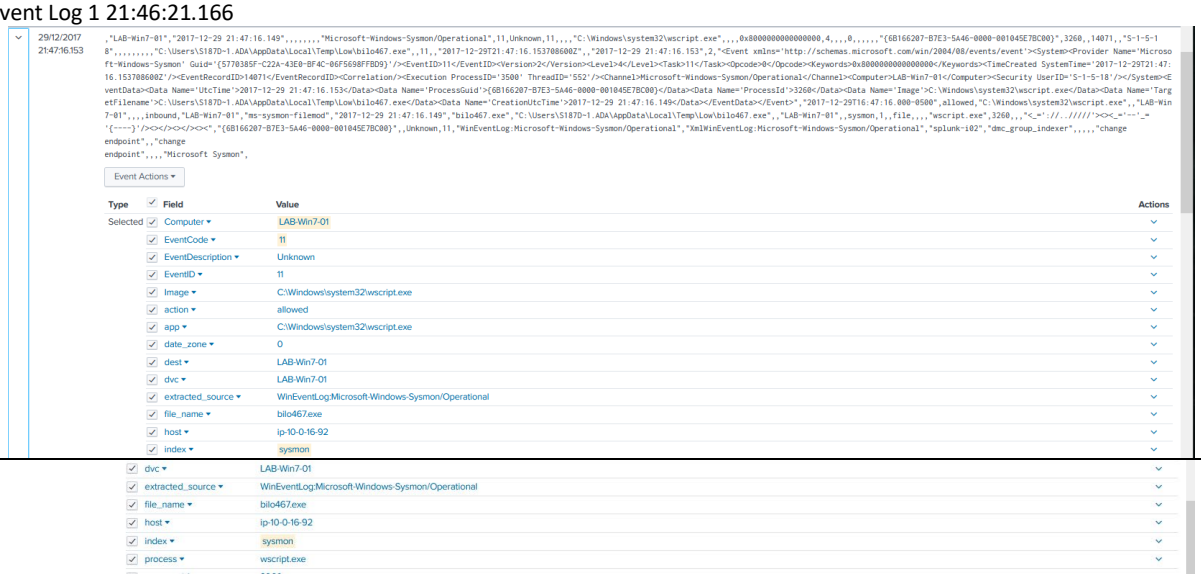
Select Event ID 11



With the Event ID 11 there are now a total of 4 events
Investigate the individual logs

Select the drop-down arrow for each log and investigate findings / fields listed

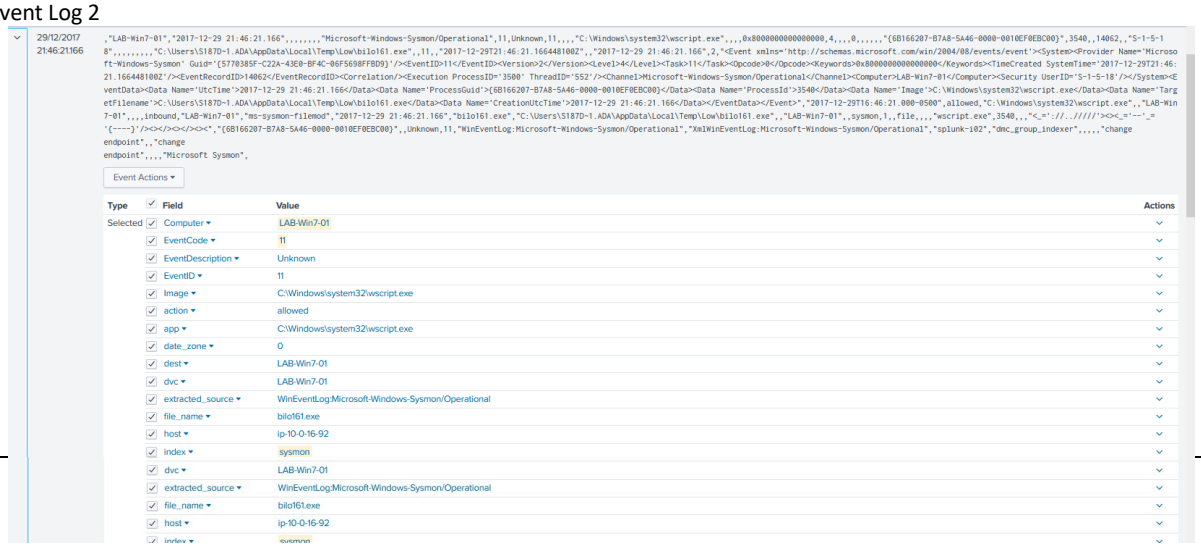
Event Log 1 21:46:21.166



A suspicious file name is evident (Bilo467.exe)

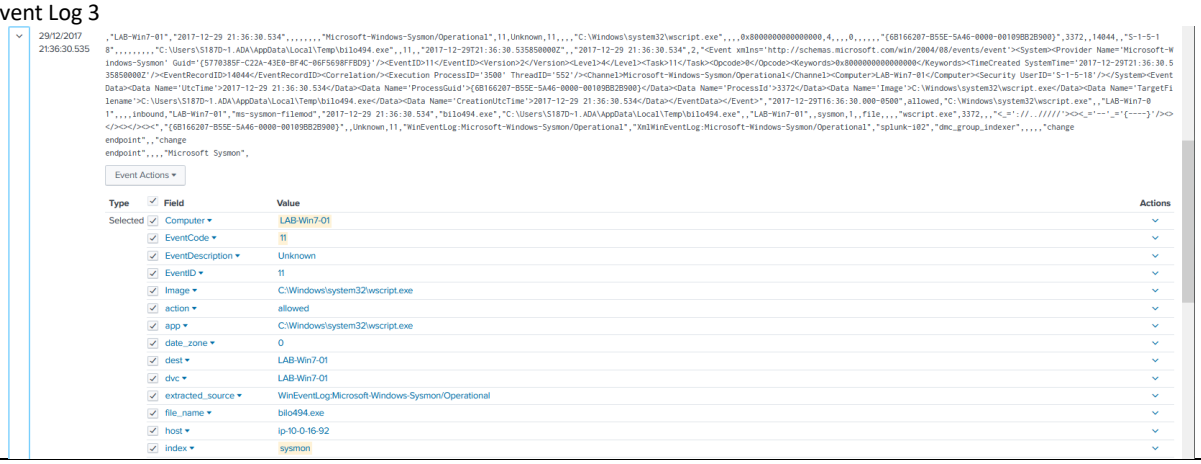
This is hidden data…this is the type of spurious location to look for when hunting a EK file

Event Log 2



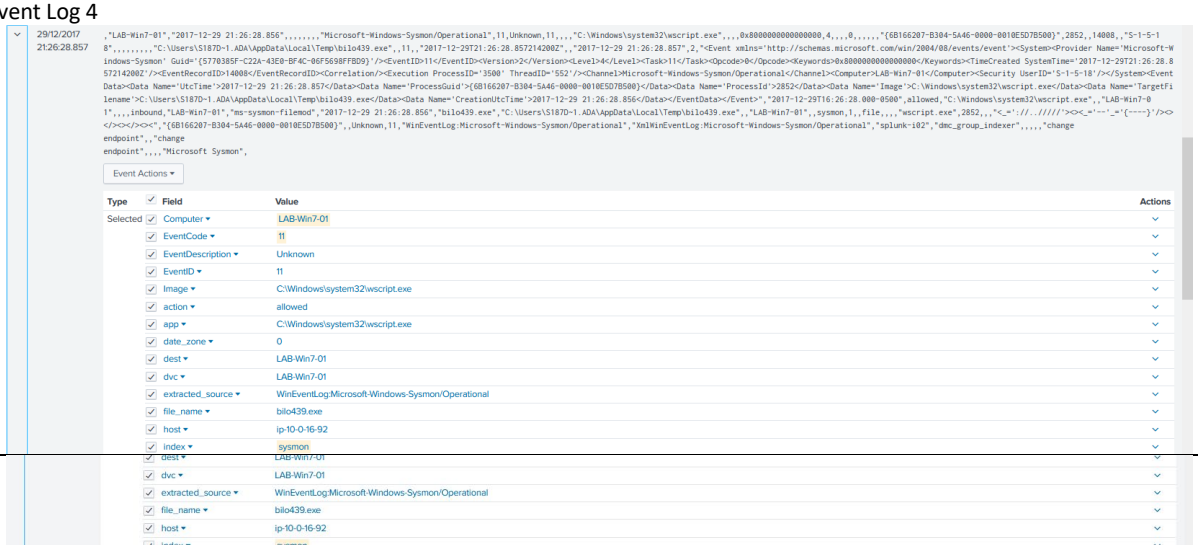
A suspicious file name is evident (Bilo161.exe)

Event Log 3



A suspicious file name is evident (Bilo494.exe)

Event Log 4



A suspicious file name is evident (Bilo439.exe)

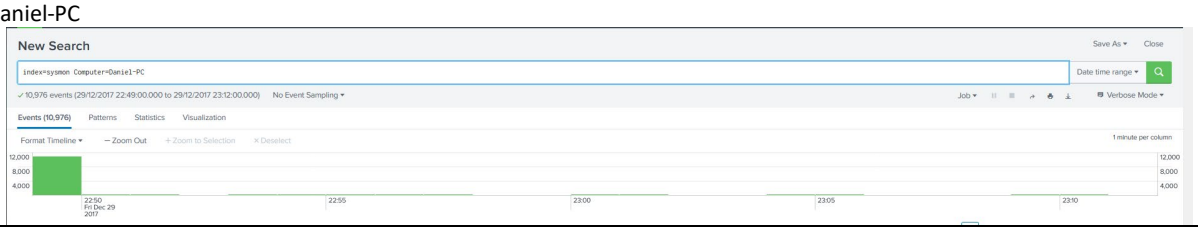
Now investigate the remaining computers for similar file names

10.5.10.130 - Daniel-PC – Daniel

10.5.10.128 - LAB-Win10-03 – M. Land

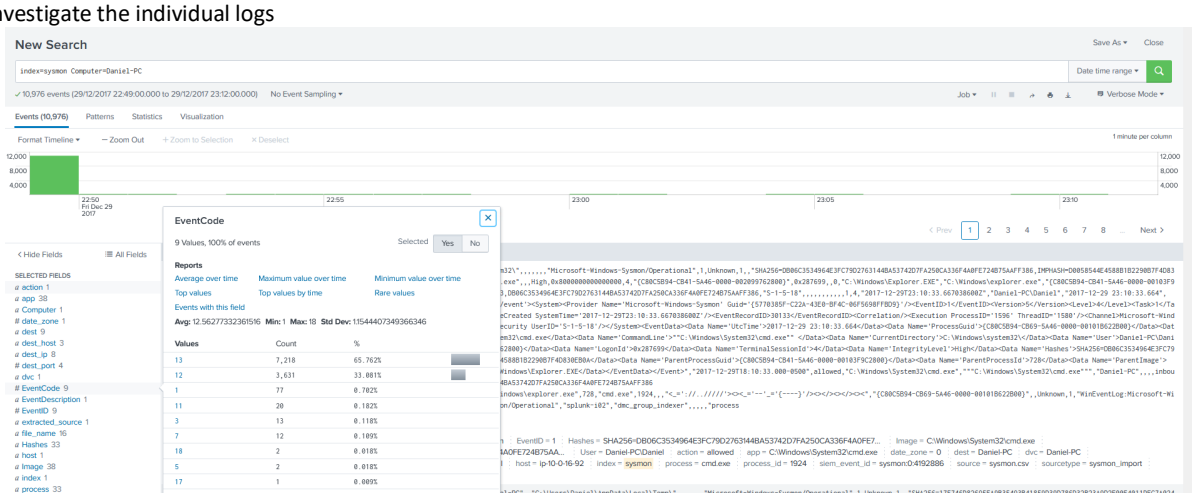
10.5.10.127 - LAB-Win10-02 – D. Walker

Daniel-PC



Event Code 11 has a total of 20 events

Investigate the individual logs



Select the Code and investigate each drop-down Event Log as before drop-down arrow for each log and investigate findings / fields listed

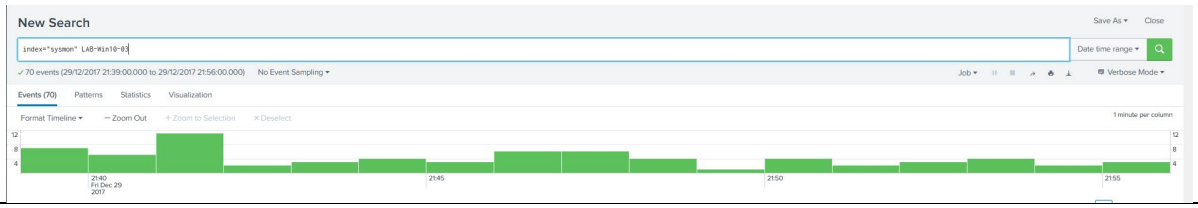
Investigate each event log for anything suspicious. (see below as examples)

Event Logs 1 and 2 show nothing suspicious

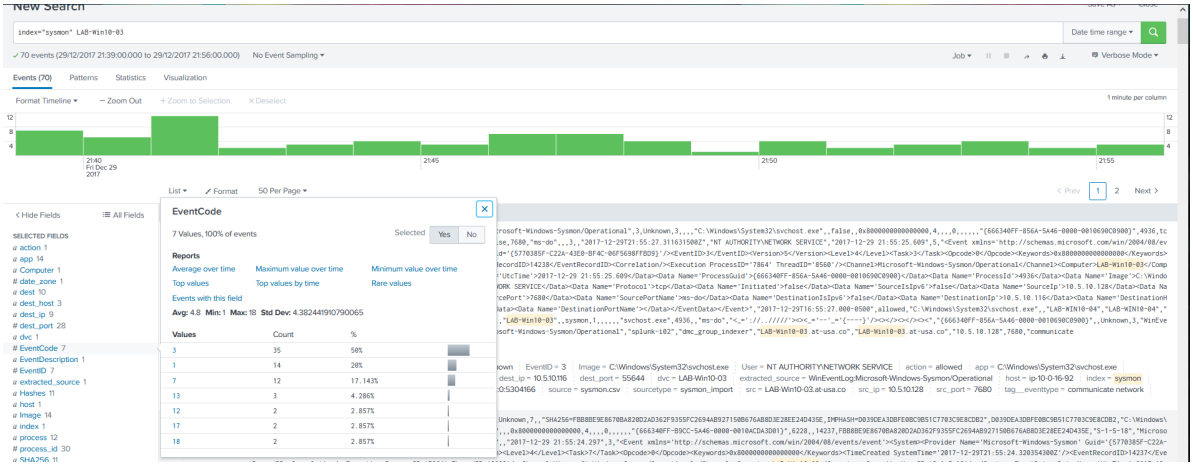
Event Log 3 has a suspicious file name

Event Log 4 has a suspicious file name

LAB-Win10-03



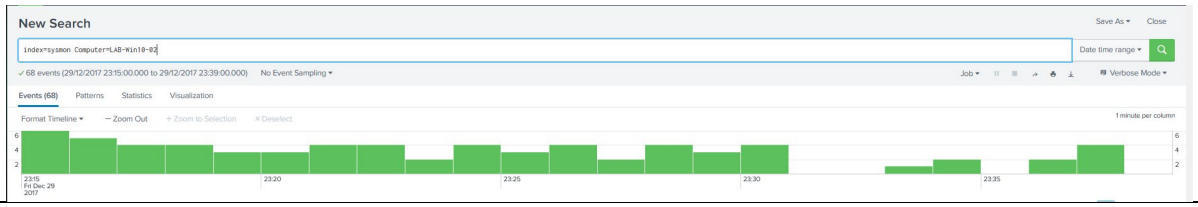
Event Code



There isn't an Event Code 11 on this device…

There were no files created on this device…

LAB-Win10-02



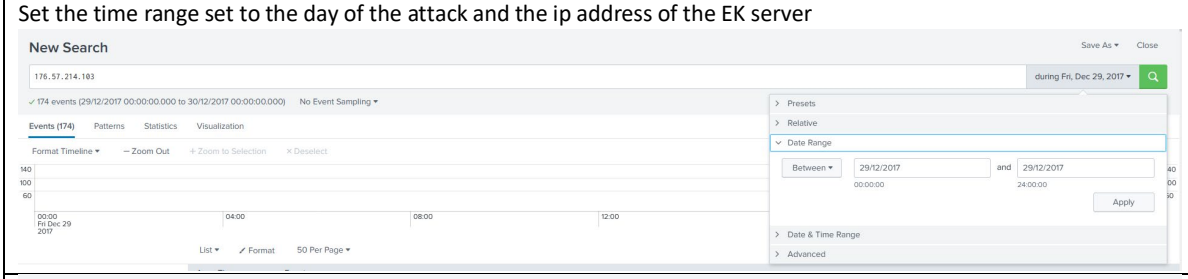
Event Code

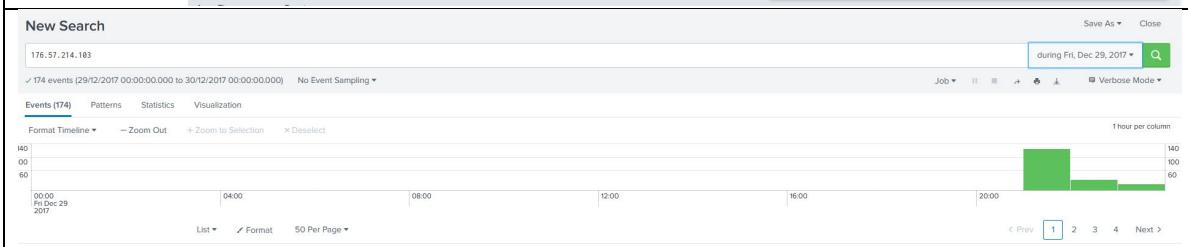
There isn't an Event Code 11 on this device…
There were no files created on this device…

4 - TIME RANGES

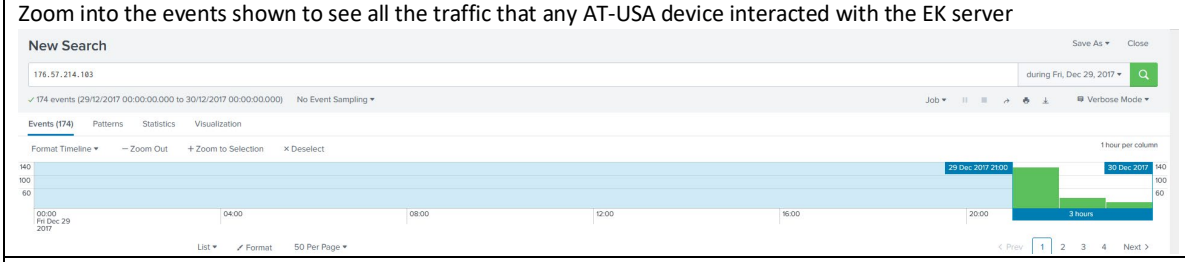
The time range during which any AT-USA devices were exposed to the threat associated with ciso[.]guide (the EK landing page)

Set the time range set to the day of the attack and the ip address of the EK server

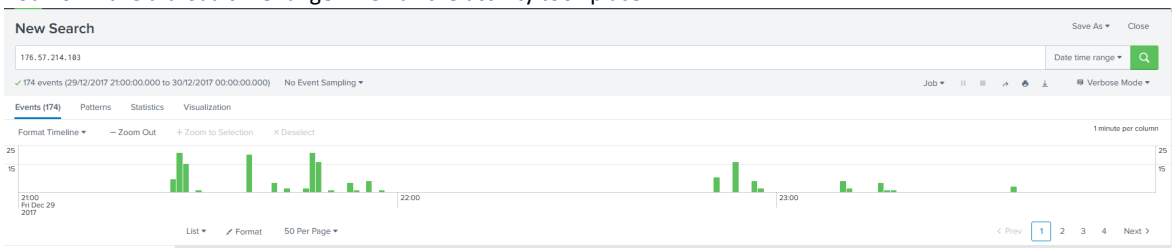




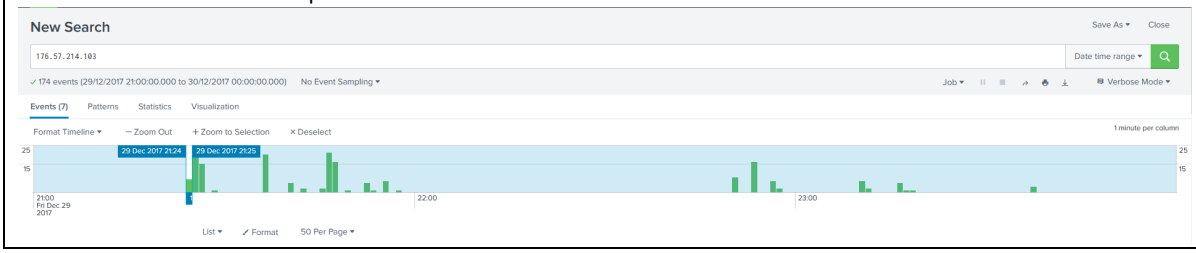
Zoom into the events shown to see all the traffic that any AT-USA device interacted with the EK server

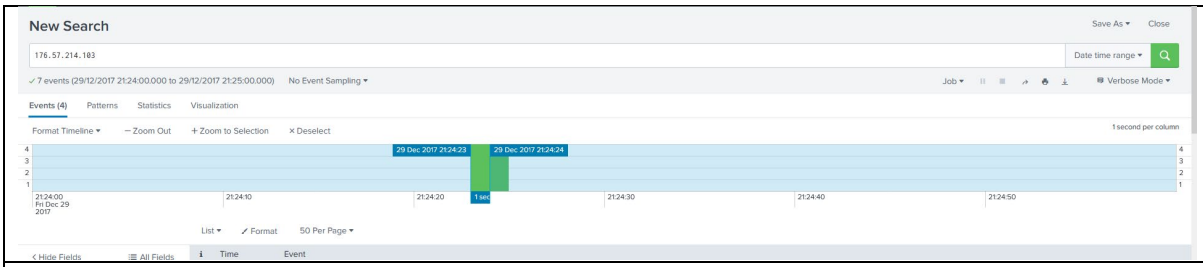


You now have a broad time range when all the activity took place



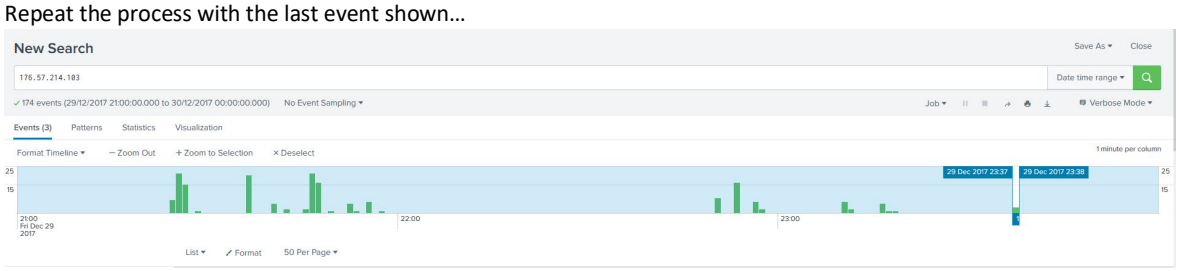
Zoom into the first and last events shown to get your full-time range of the EK events, then you can single out each device to establish each own time stamps.

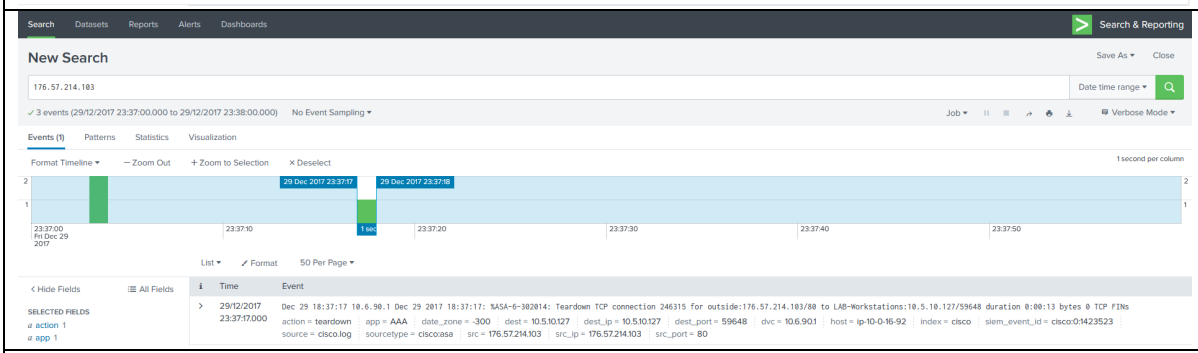




First event took place at 21:24:23.000

Repeat the process with the last event shown…

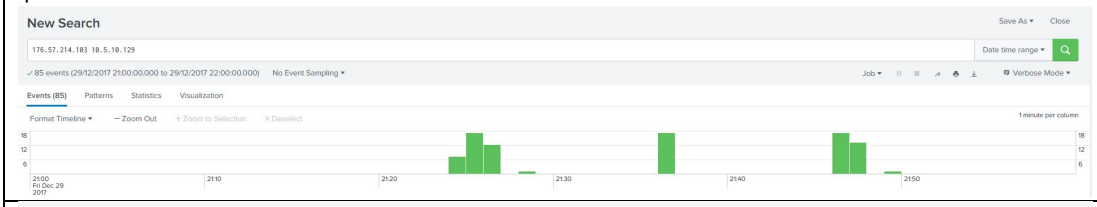


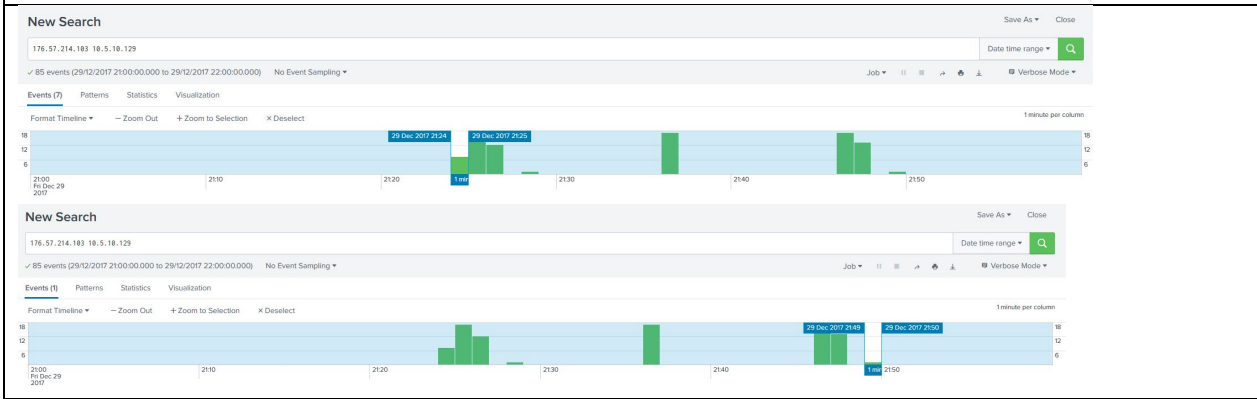


The last EK event took place at 23:37:17.000

Now search each device ‘s interactions with the EK server

ip=10.5.10.129

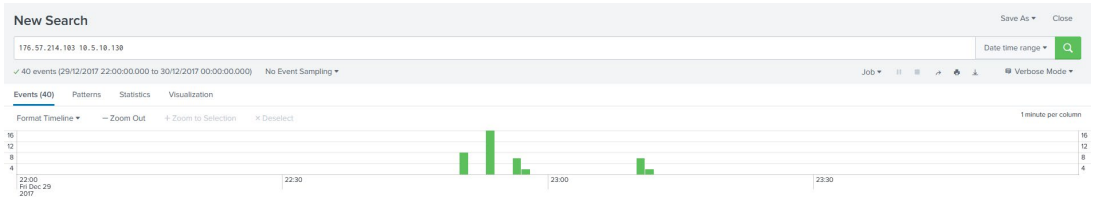


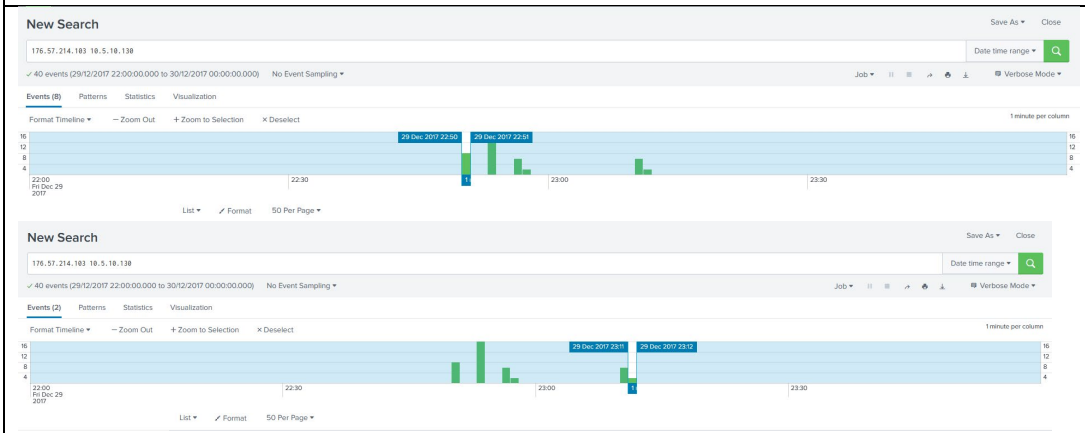


First interaction is at 21:24:23.000

Last interaction is at 21:49:14.000

ip=10.5.10.130

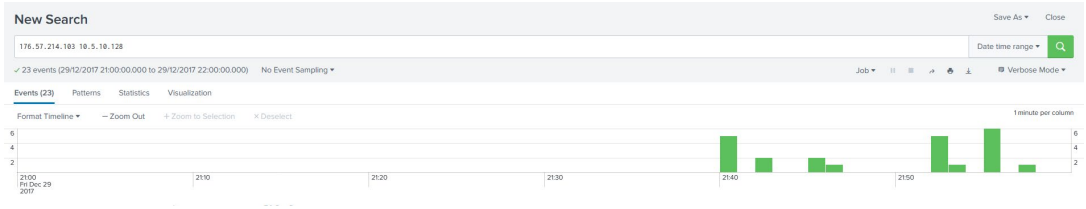


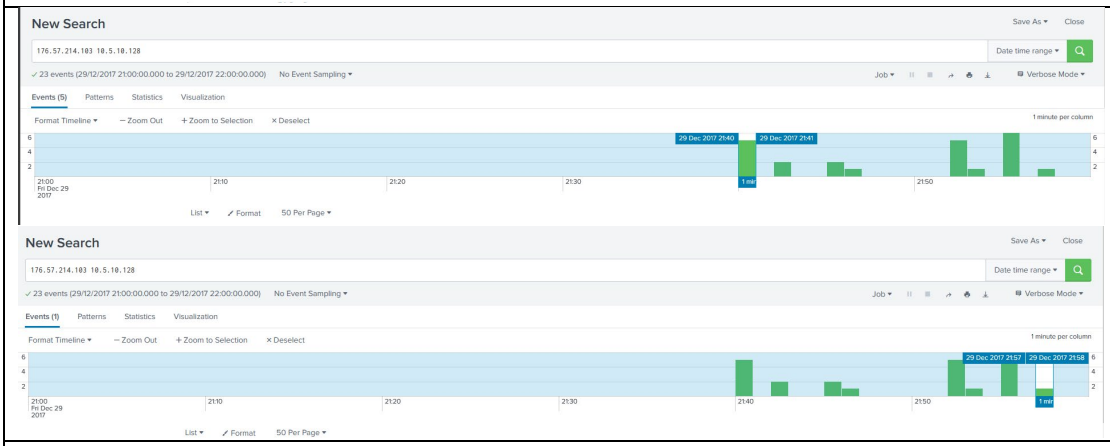


First interaction is at 22:50:07.000

Last interaction is at 23:11:16.000

ip=10.5.10.128

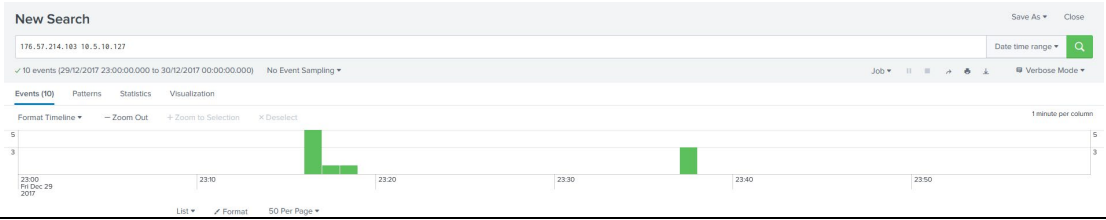


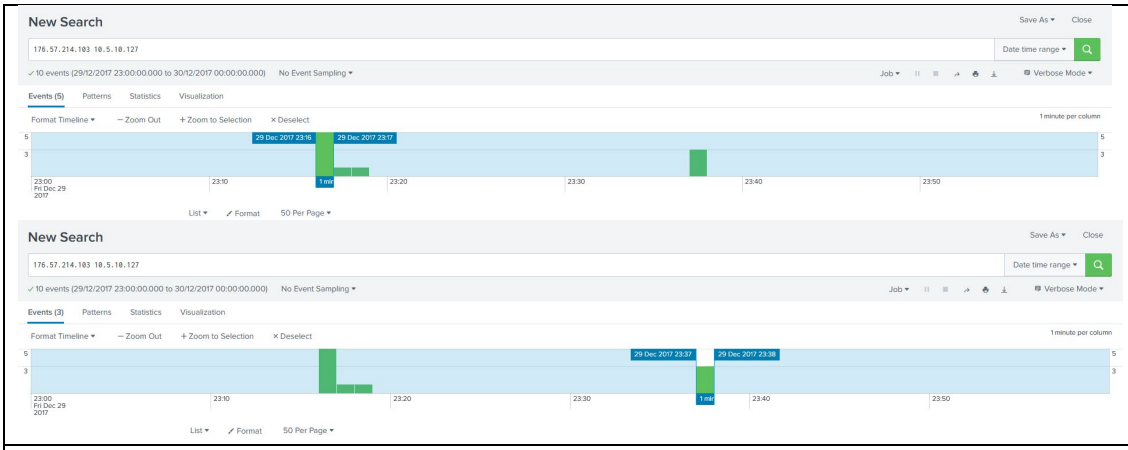


First interaction is at 21:40:33.000

Last interaction is at 21:57:06.000

ip=10.5.10.127





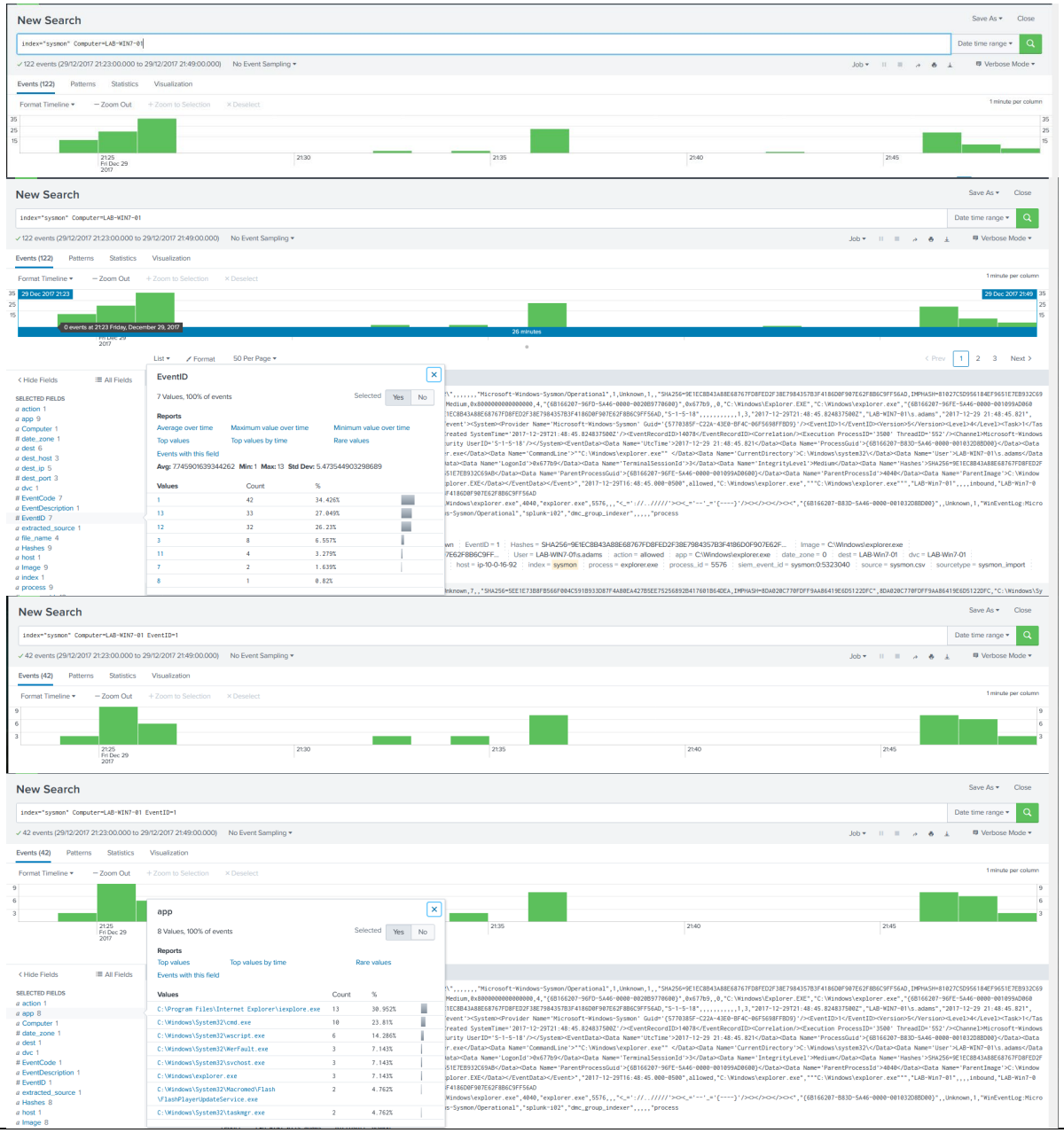
First interaction is at 23:16:10.000
Last interaction is at 23:37:17.000

5 - EVENT ID 1 – PROCESS CREATION

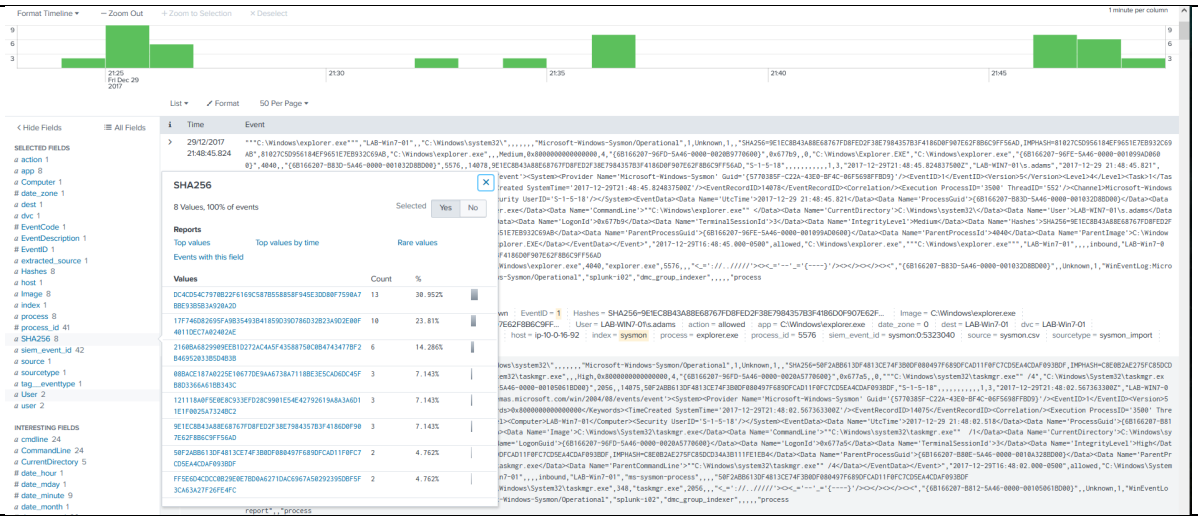
Event ID 1: Process creation

The process creation event provides extended information about a newly created process. The full command line provides context on the process execution. The `ProcessGUID` field is a unique value for this process across a domain to make event correlation easier. The hash is a full hash of the file with the algorithms in the `HashType` field.

LAB-Win7-01

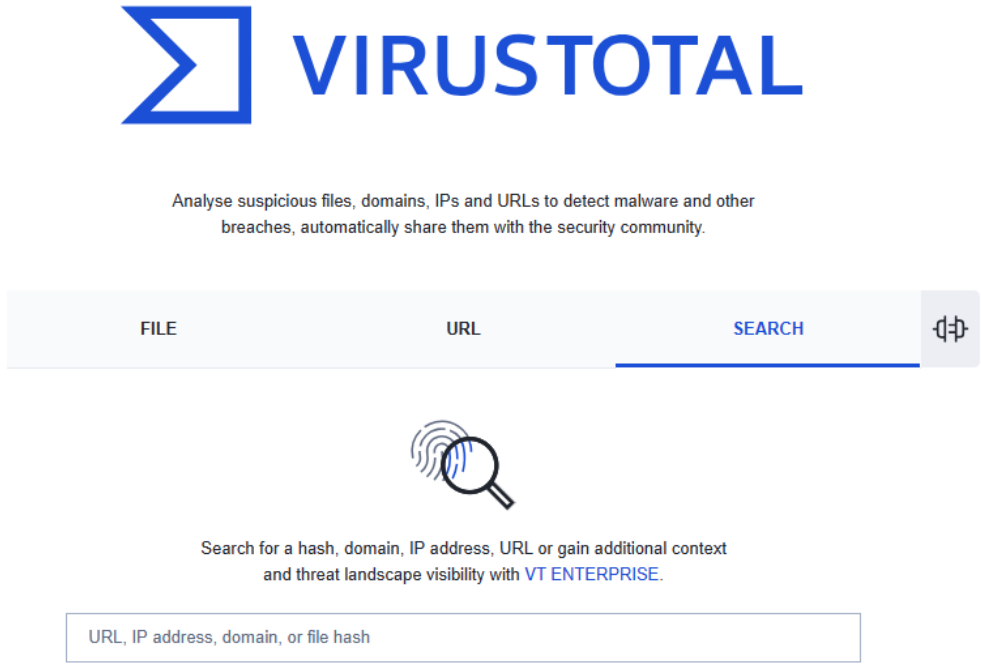


There are no bilo files in the app field, so it appears that no bilo files were executed on this device…but not definitive yet…
To help confirm there is a SHA256 / Hashes that can be searched…



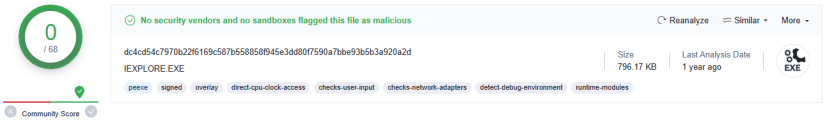
DC4CD54C7970B22F6169C587B558858F945E3DD80F7590A7BBE93B5B3A920A2D

Go to Virus Total and search the different SHA256's / Hashes



1st SHA256

DC4CD54C7970B22F6169C587B558858F945E3DD80F7590A7BBE93B5B3A920A2D

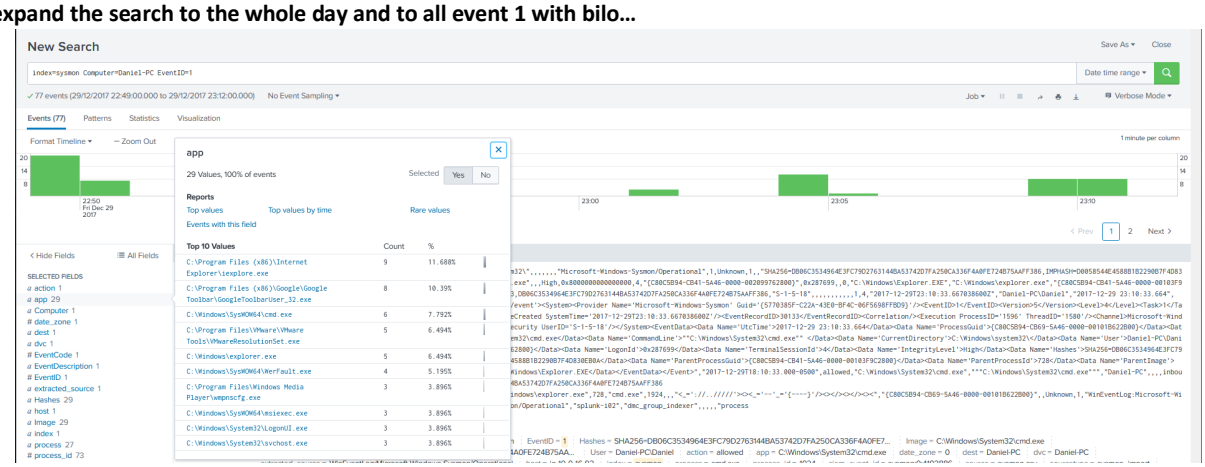


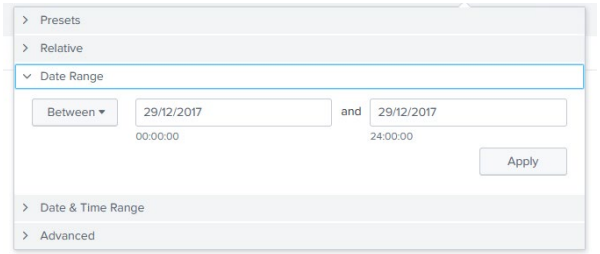
This is a safe hash

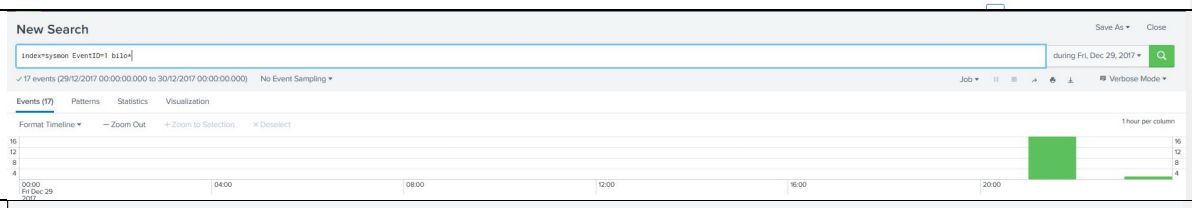
Continue to investigate the remaining hashes.

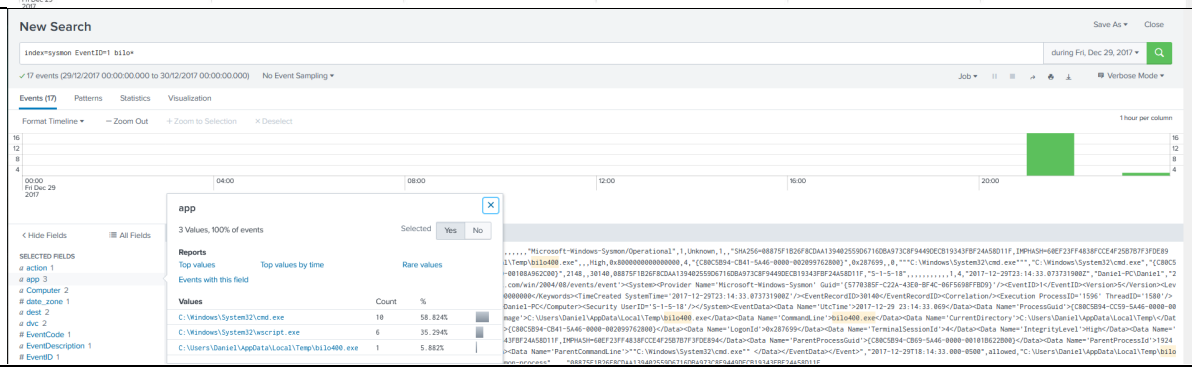
LAB-Win7-01 appears to have been compromised by the EK (Rig)…
The Payloads were successfully delivered, but the device was not compromised by the malware (Ramnit)…

When trying to search in the current timeline on Daniel-PC there doesn't appear to be any events associated with bilo…so expand the search to the whole day and to all event 1 with bilo…

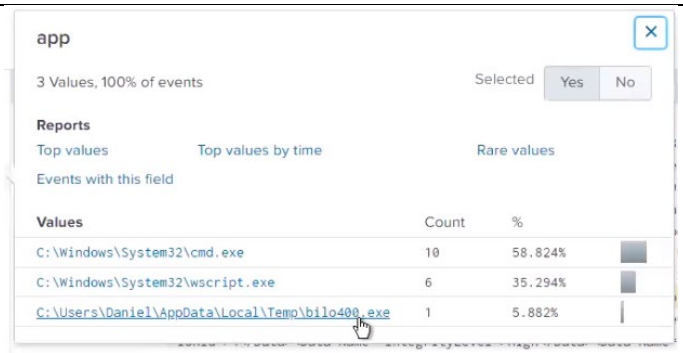




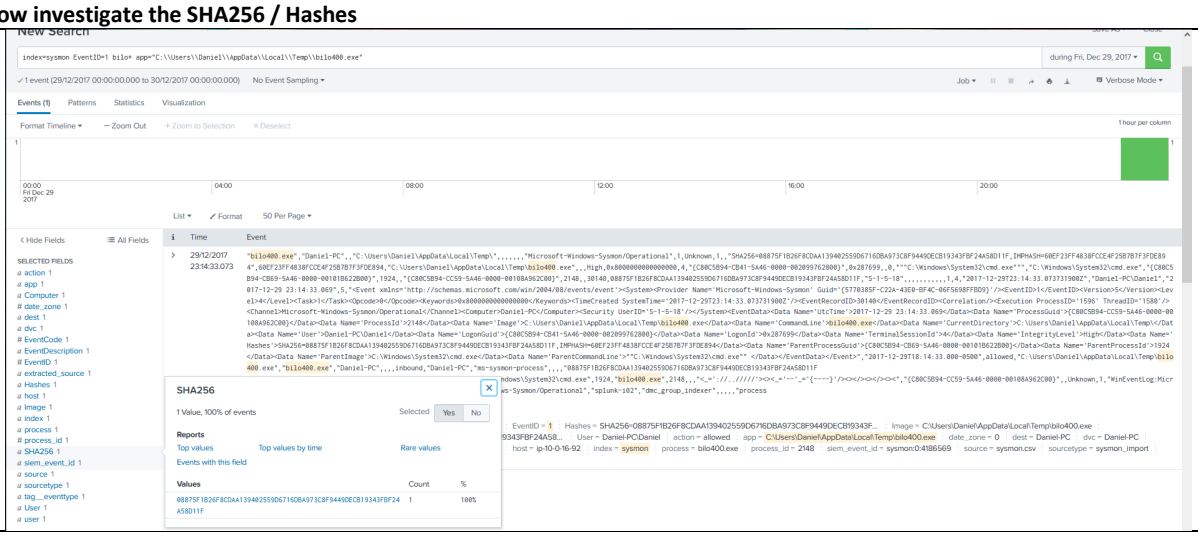


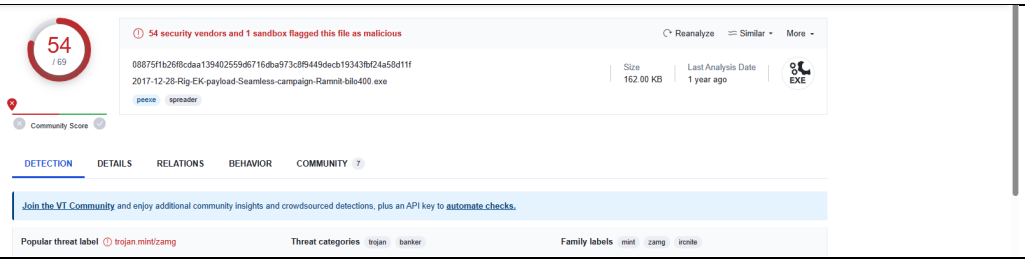


Select the appropriate app and add to search



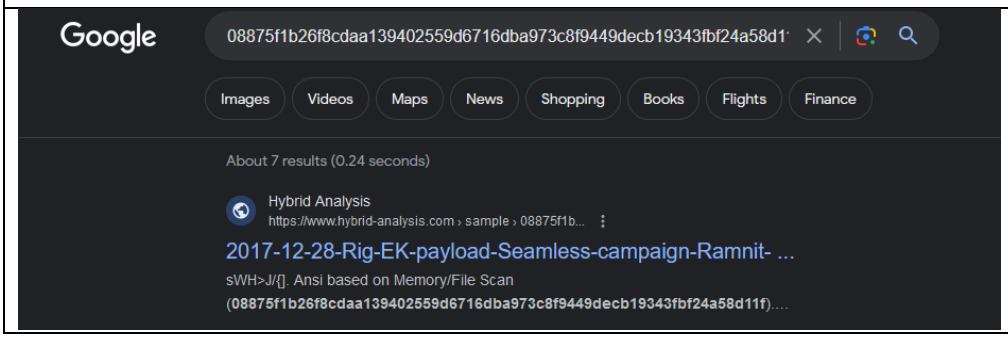
Now investigate the SHA256 / Hashes

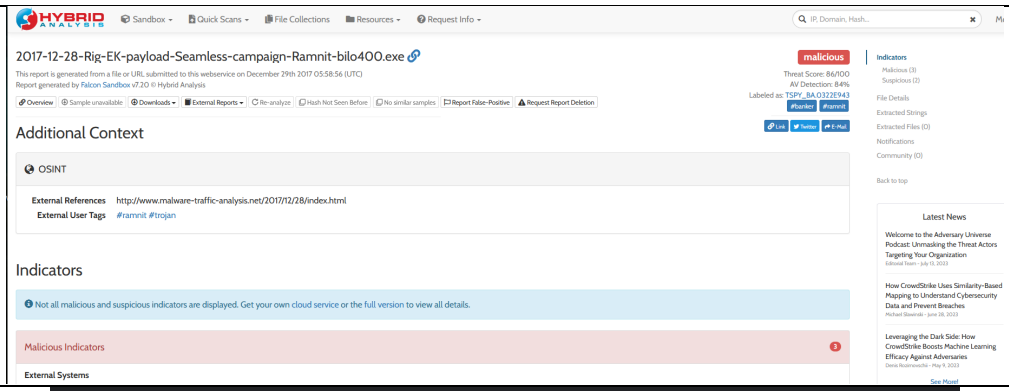


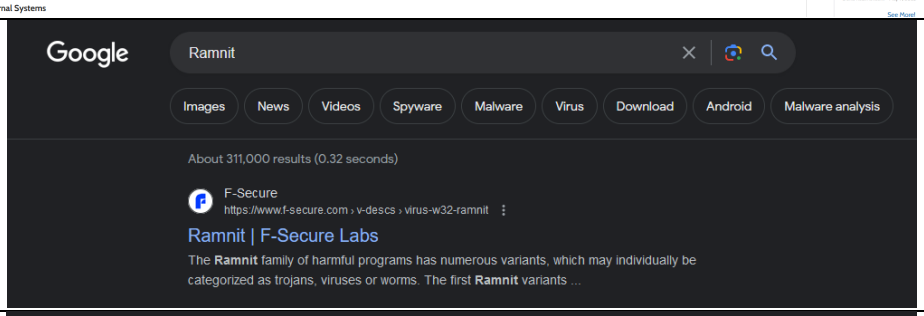


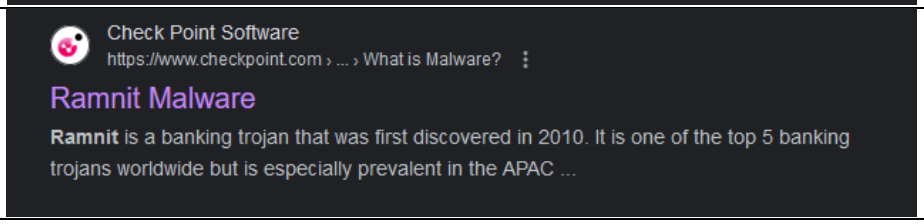
The bilo files are payloads
The threat catagories are trojan and banker

Perform a google search for the hash…
08875f1b26f8cdaa139402559d6716dba973c8f9449decb19343fbf24a58d11f









How the Malware Works

Ramnit is a banking trojan, meaning that it is primarily intended to steal account credentials for online banking. However, like many banking trojans, Ramnit is designed to be highly modular, enabling it to collect additional types of credentials such as those for social media, email, and other accounts or to download and deploy other malware.

Ramnit is often spread via phishing campaigns that may deploy multi-stage malware. Once the target falls for the initial phishing campaign and runs the malware, it downloads and executes additional malware that eventually launches the Ramnit trojan. Ramnit will then attempt to collect banking credentials and may download additional Ramnit modules or other malware to achieve the attacker's goals.

One of the distinguishing features of the Ramnit malware is the use of both hardcoded domains and a domain generation algorithm (DGA) for command and control. Malware using a DGA generates a sequence of random-looking domains to which it sends command and control traffic. The attacker's command and control server runs the same DGA and registers these domains, directing the traffic to the attacker-controlled system. By using a DGA, the malware can avoid DNS blocklists because it is constantly using new, unblocked domains for its traffic.

The Threat

Since Ramnit is a modular banking trojan, the primary threat of the malware is the loss of an individual's login credentials for online banking, which may result in the theft of funds or the user's identity.

However, the Ramnit malware also can deploy additional modules or be used as a delivery vector for other malware variants. This means that the impact of a Ramnit infection depends on the details of the attack campaign and the malicious functionality that is successfully executed on the infected device.

Target Industries

Ramnit is primarily a banking trojan, meaning that its purpose is to steal login credentials for online banking, which cybercriminals can sell or use in future attacks. For this reason, Ramnit primarily targets individuals rather than focusing on particular industries.

Ramnit campaigns have been observed to target organizations in particular industries. For example, a 2019 campaign targeted financial organizations in the United Kingdom, Italy, and Canada.

How to Protect Against Ramnit Malware

Some best practices for protecting against the Ramnit banking trojan include:

- **Anti-Phishing Protection**: Ramnit malware is usually delivered as a malicious attachment to a phishing email, often via a downloader. Anti-phishing protections can help to identify and block or sanitize this malicious content, preventing the malware from reaching the user's device.
- **Endpoint Security Solutions**: Ramnit is an established malware variant with well-known behaviors and features. An endpoint security solution provides an organization or individual with the ability to detect Ramnit infections and prevent them from stealing credentials or deploying additional malware.
- **Cybersecurity Awareness Training**: Ramnit is commonly deployed via phishing emails, relying on deception to trick the user into executing the malicious functionality. Training employees to recognize and properly respond to phishing attacks can help prevent Ramnit infections.
- **DNS Traffic Analysis**: Ramnit malware often uses a DGA, which generates a series of random domains for command and control communications. Analysis of domain name lookups on a DNS server can enable an organization to identify the suspicious domain names that may indicate a Ramnit infection.
- **Multi-Factor Authentication (MFA)**: Implementing MFA makes it more difficult for an attacker to make use of these stolen credentials by requiring access to an additional authentication factor.
- **Zero Trust Security**: While Ramnit primarily is designed to steal online banking credentials, it can also steal other credentials. By implementing a zero trust security policy and limiting the access and permissions of user accounts, an organization can decrease the potential impact and damage caused by a compromised account.

Ramnit Malware Detection and Protection with Check Point

Ramnit is one of the leading banking trojans and a common malware variant, especially in the APAC region. However, it is only one of several cybersecurity threats that companies face. For more information about the leading malware threats and the current cyber threat landscape, check out Check Point's 2023 Cyber Security Report.

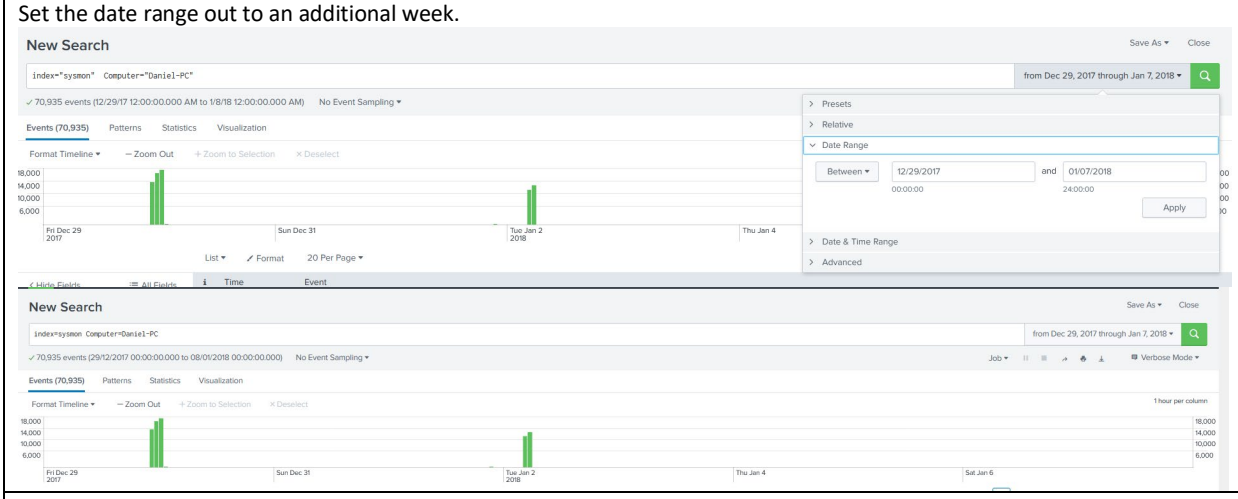
Check Point Harmony Endpoint offers comprehensive threat prevention and detection for Ramnit, other malware, and various threats to the security of an organization's endpoints. For more information about Harmony Endpoint and to learn how it can help to enhance your organization's malware threat prevention capabilities, sign up for a free demo today.

Sumation of Event 1 on the 4 devices:

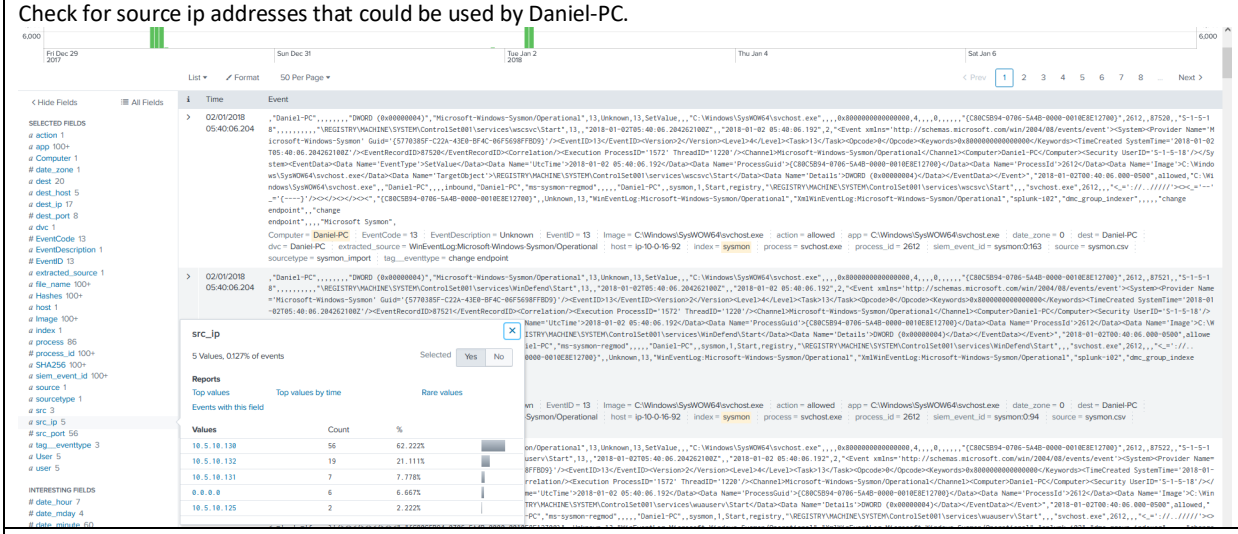
1. **LAB-Win10-02 shows no signs of the EK (Rig) or any payloads for the Malware Ramnit.**
2. **LAB-Win10-03 shows no signs of the EK (Rig) or any payloads for the Malware Ramnit.**
3. **LAB-Win7-01 - appears to have been compromised by the EK (Rig)…The Payloads were successfully delivered, but the device was not compromised by the malware Ramnit.**
4. **Daniel-PC has been compromised by the EK (Rig)…The Payloads were successfully delivered, and the device was infected by the malware Ramnit.**

6 - C2 TRAFFIC

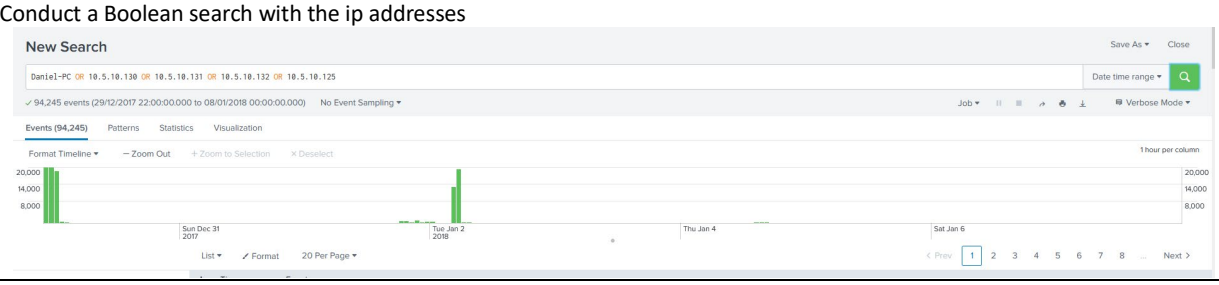
Set the date range out to an additional week.



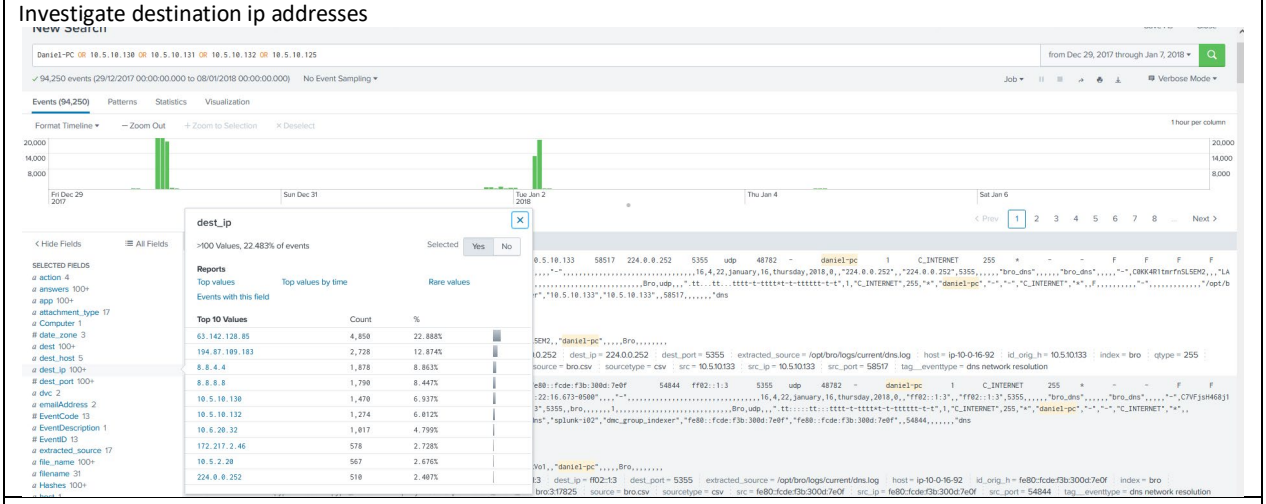
Check for source ip addresses that could be used by Daniel-PC.



Conduct a Boolean search with the ip addresses

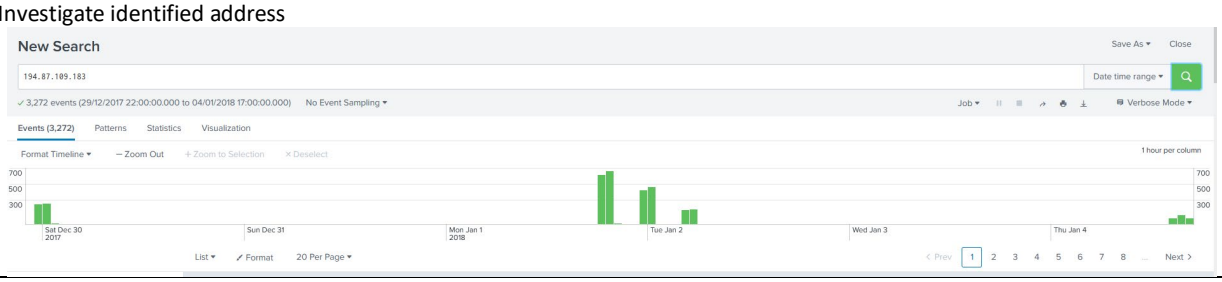


Investigate destination ip addresses

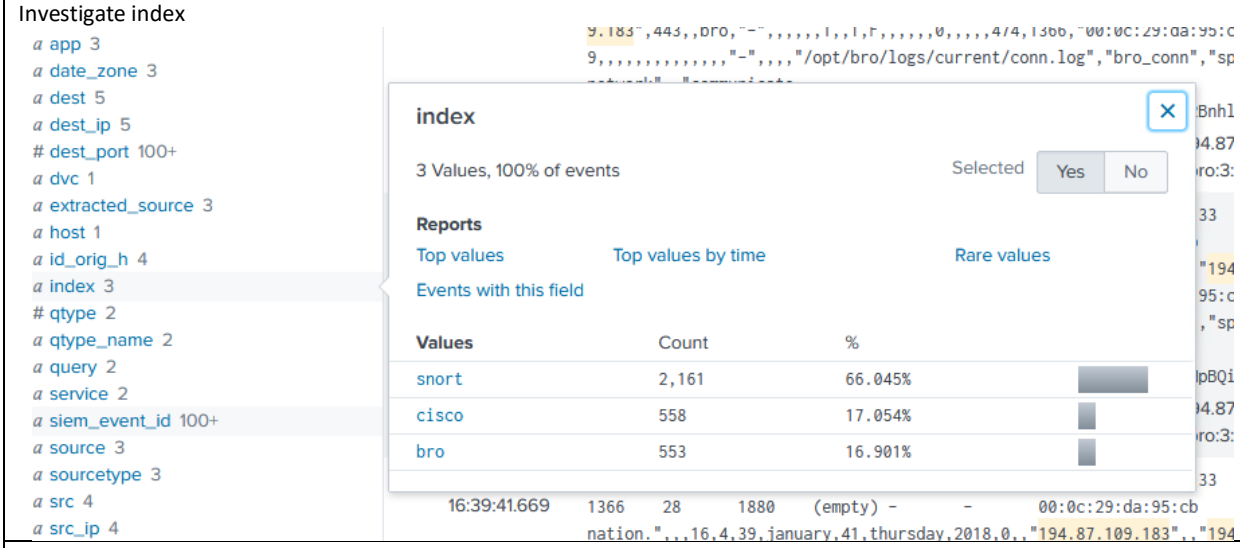


Conduct a Google search of unknown addresses

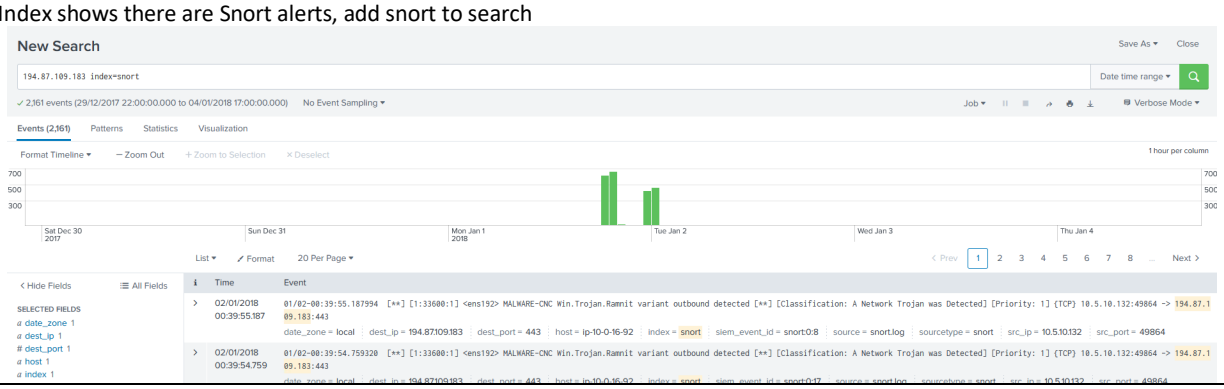
Investigate identified address



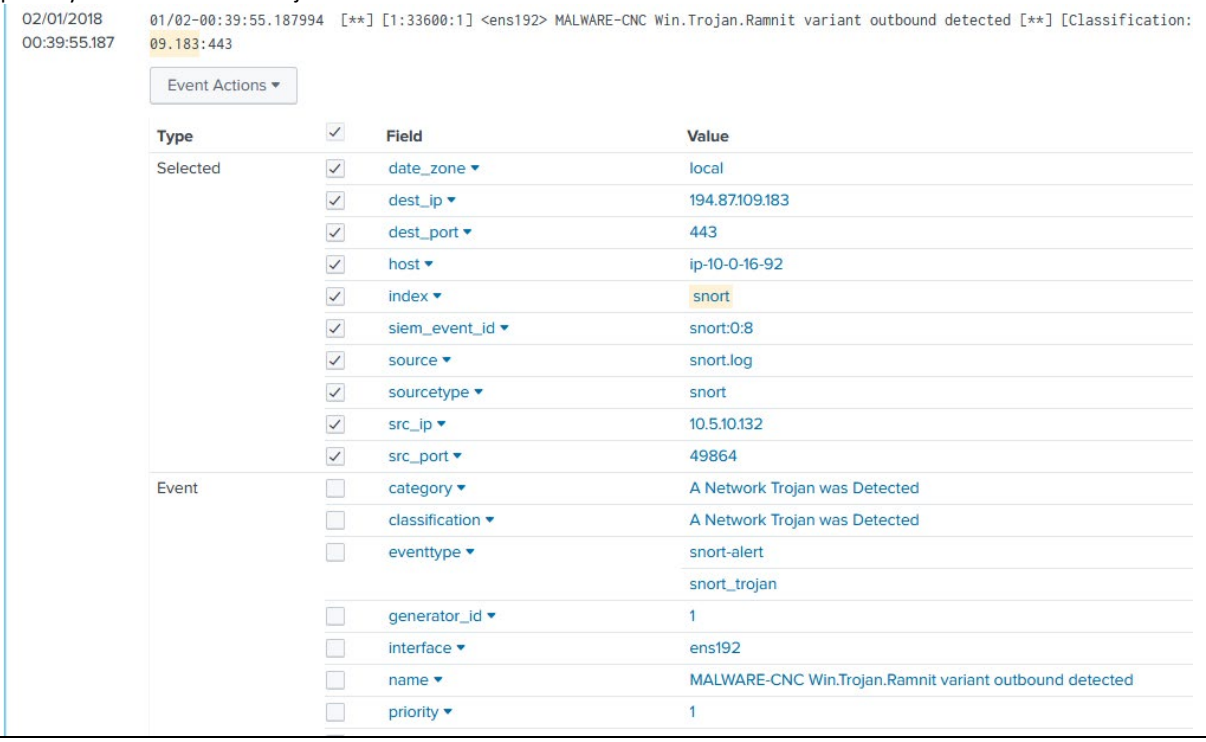
Investigate index



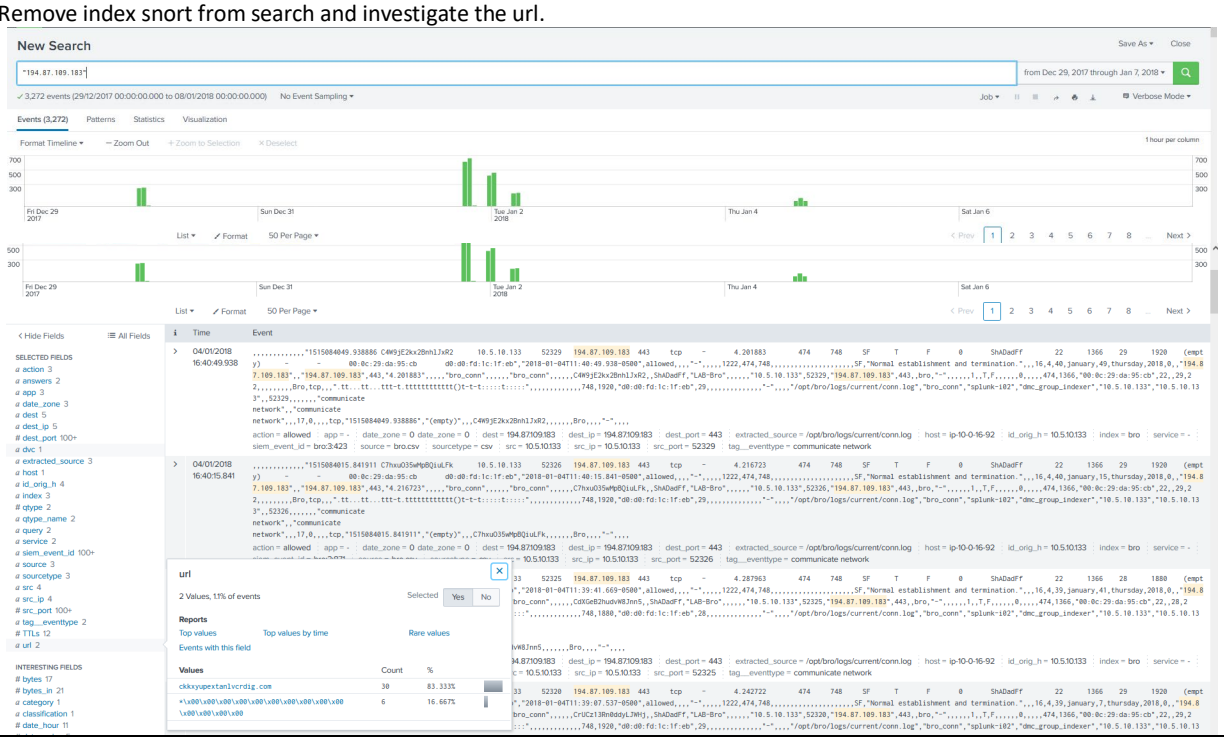
Index shows there are Snort alerts, add snort to search



Open any alert and it shows Trojan detected.

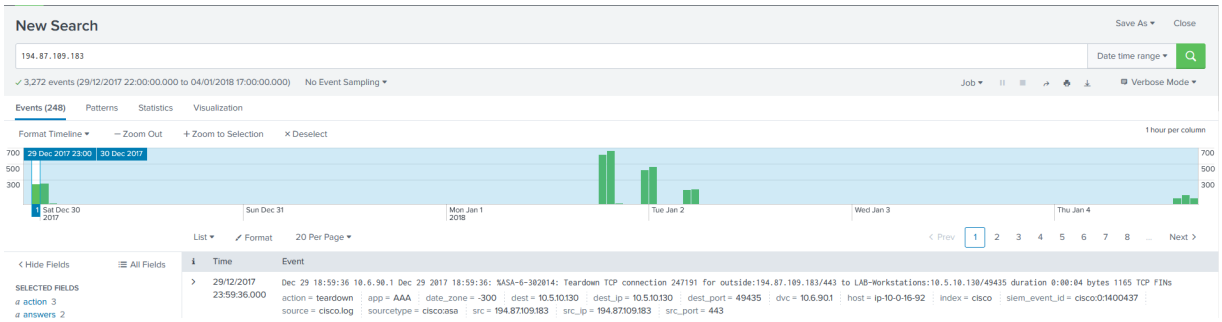


Remove index snort from search and investigate the url.

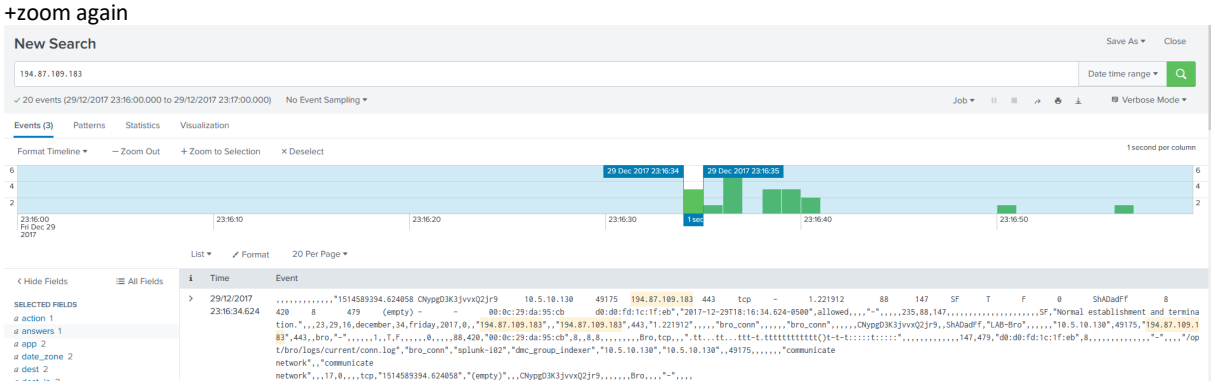


url shows a suspicious domain name.
ckkxyupextanlvcrdig.com

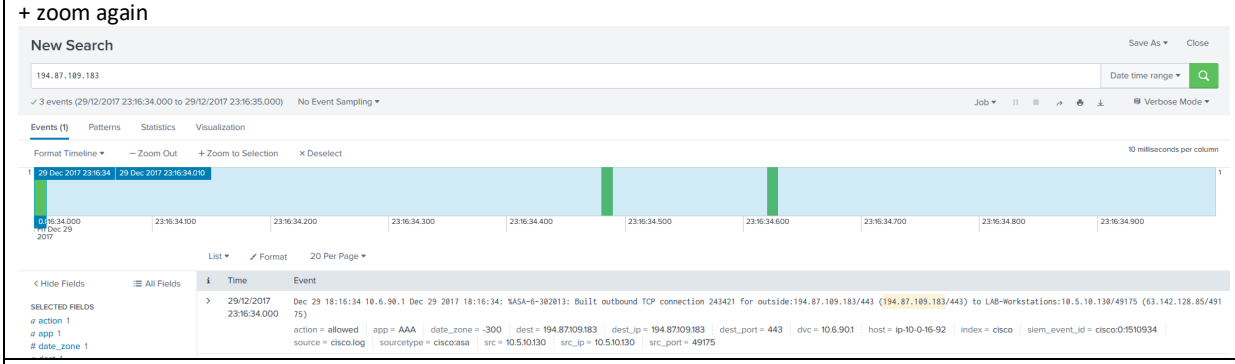
To establish first contact start on first block and +zoom.



+zoom again

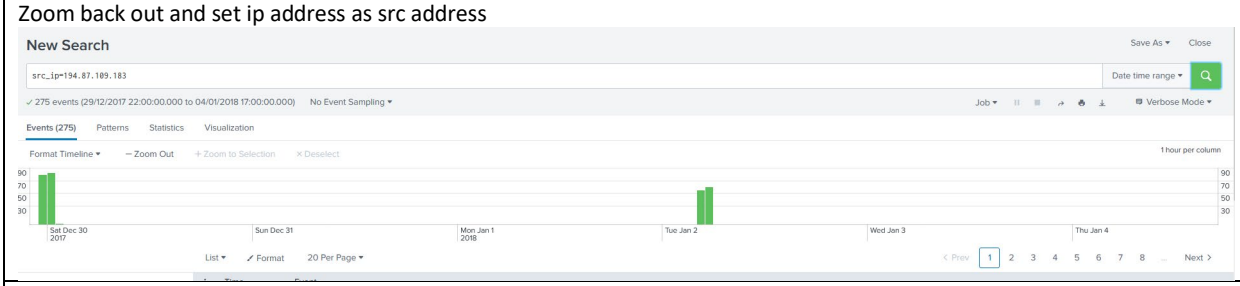


+ zoom again

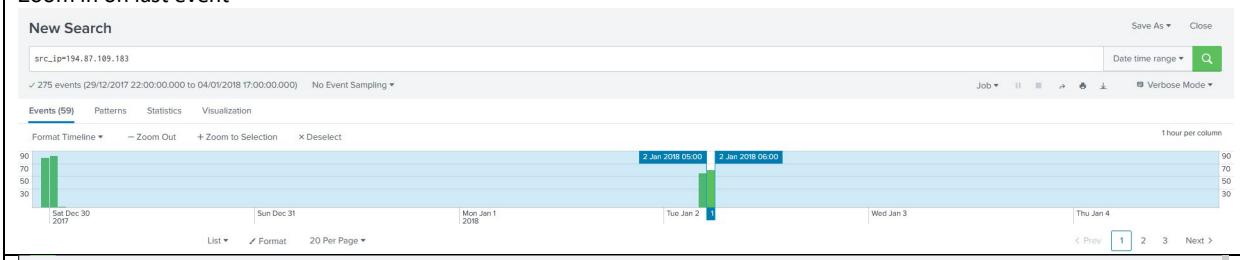


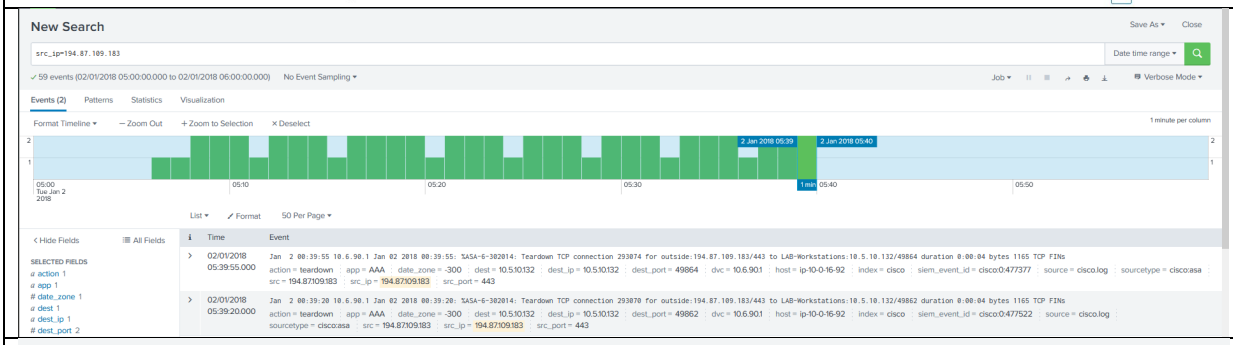
This shows the first time the device made a connection
23:16:34.000

Zoom back out and set ip address as src address



Zoom in on last event

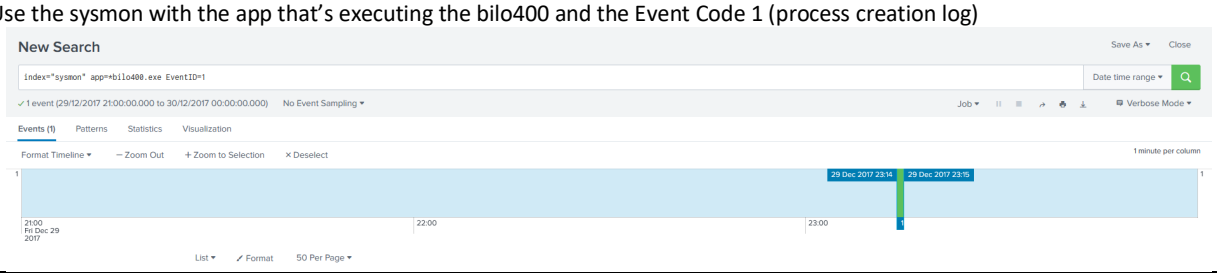




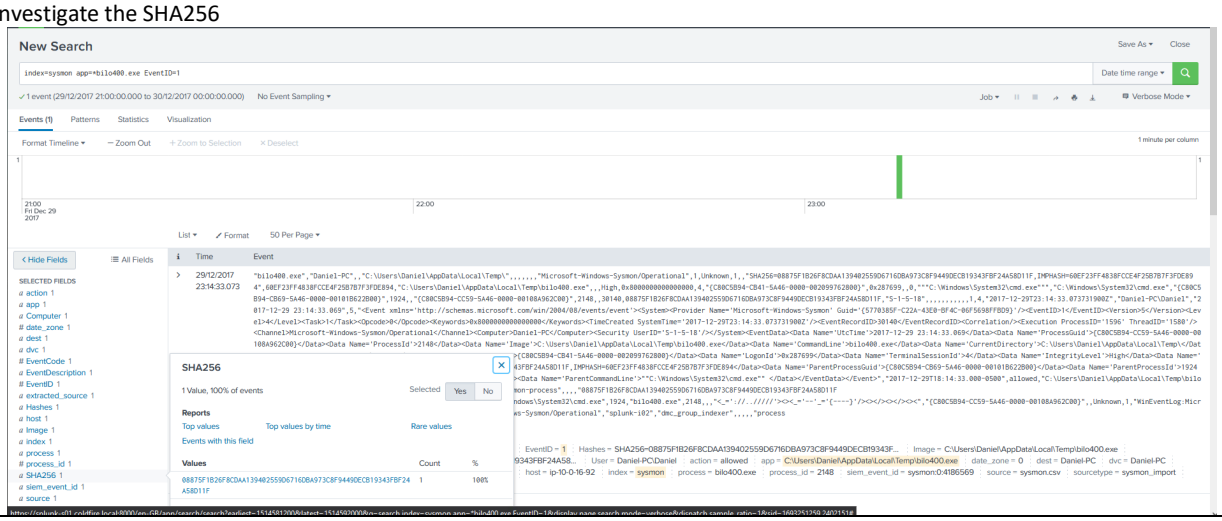
Last successful comms event is at 05:39:55.000

7 - IDENTIFYING FIRST EXECUTION OF THE MALWARE BINARY

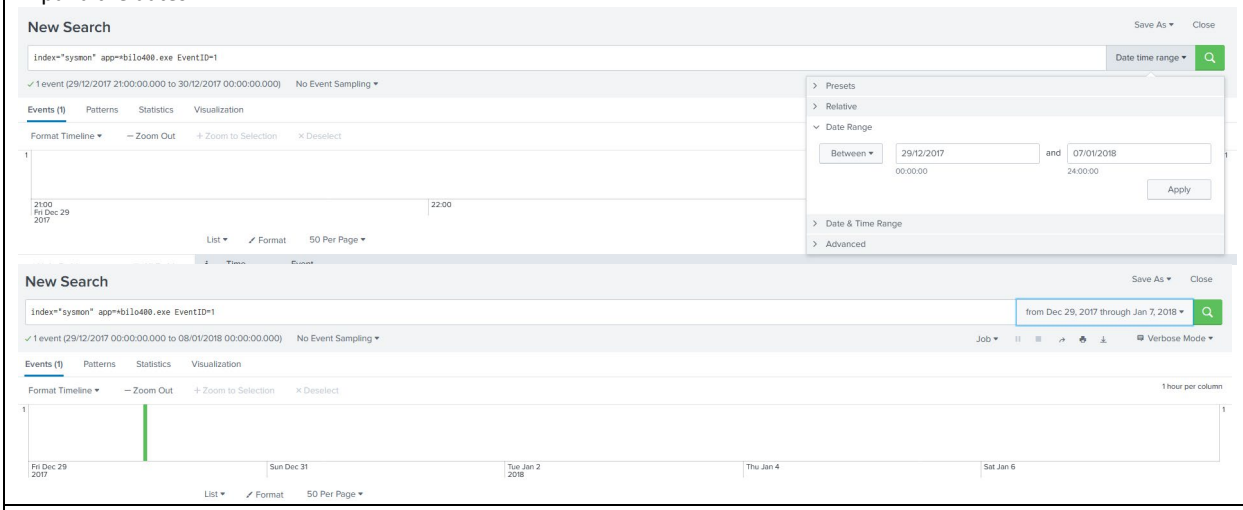
Use the sysmon with the app that's executing the bilo400 and the Event Code 1 (process creation log)



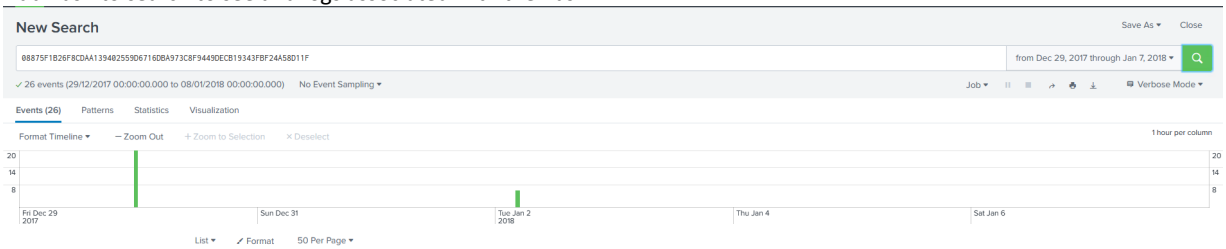
Investigate the SHA256



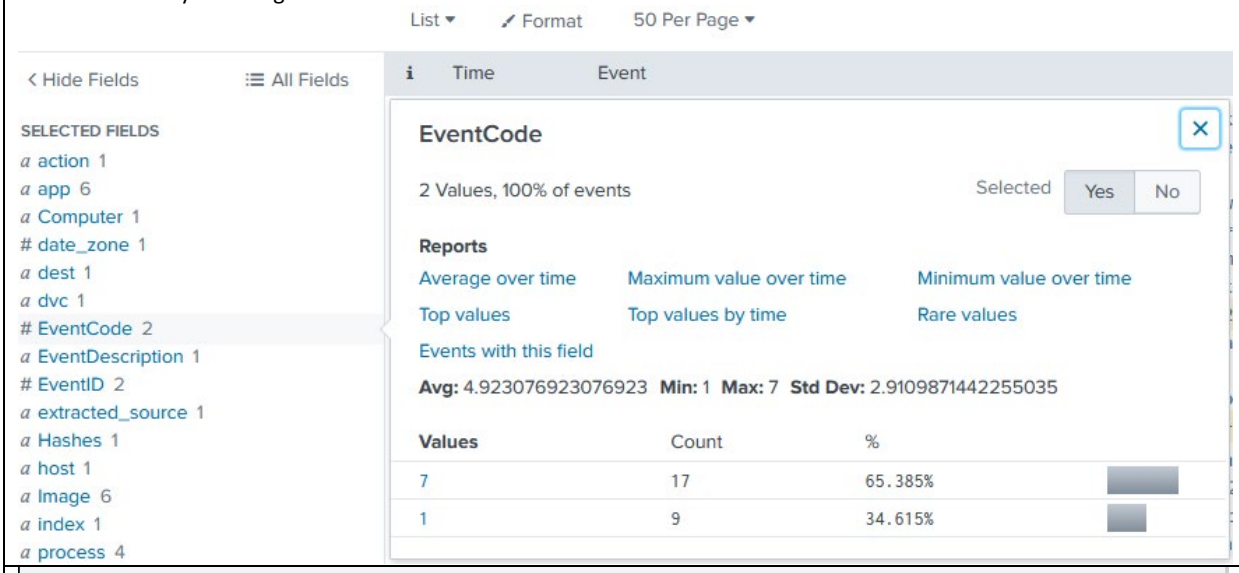
Expand the dates



Add hash to search to see and logs associated with the hash



Narrow search by including Event Code 1



There are 9 separate events which gives proof of persistence.

8 - REGISTRY EVENTS

Event ID 12: RegistryEvent (Object create and delete)

Registry key and value create and delete operations map to this event type, which can be useful for monitoring for changes to Registry autostart locations, or specific malware registry modifications.

Sysmon uses abbreviated versions of Registry root key names, with the following mappings:

Key name	Abbreviation
`HKEY_LOCAL_MACHINE`	`HKLM`
`HKEY_USERS`	`HKU`
`HKEY_LOCAL_MACHINE\System\ControlSet00x`	`HKLM\System\CurrentControlSet`
`HKEY_LOCAL_MACHINE\Classes`	`HKCR`

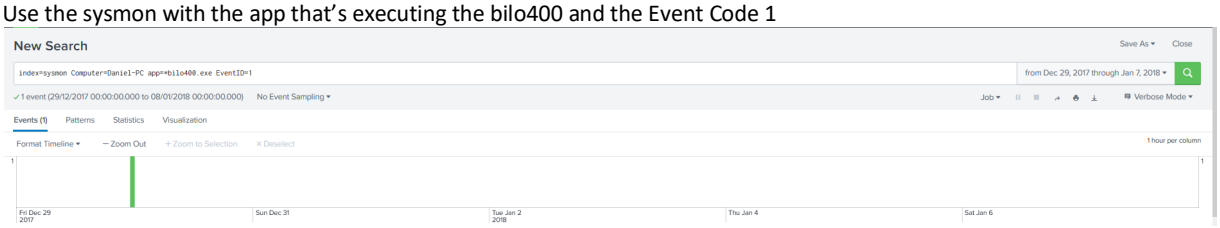
Event ID 13: RegistryEvent (Value Set)

This Registry event type identifies Registry value modifications. The event records the value written for Registry values of type `DWORD` and `QWORD`.

Event ID 14: RegistryEvent (Key and Value Rename)

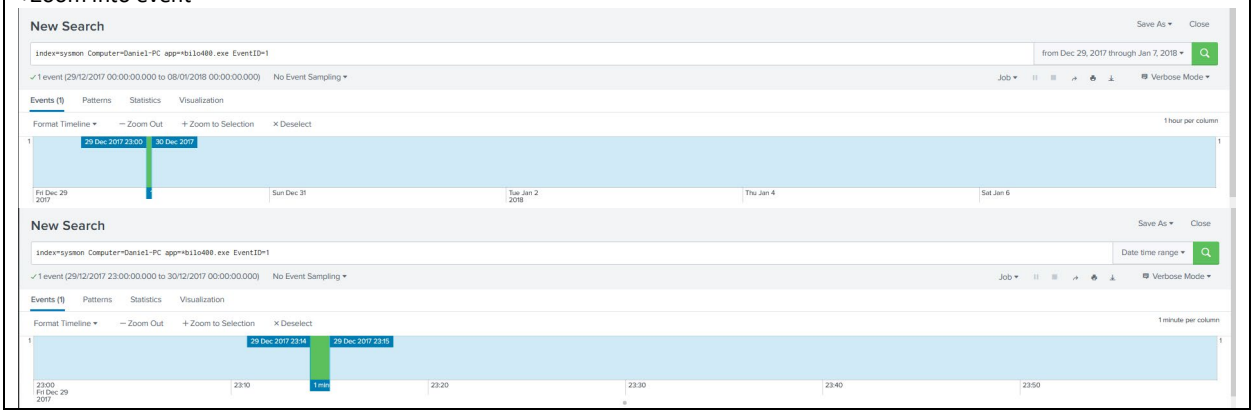
Registry key and value rename operations map to this event type, recording the new name of the key or value that was renamed.

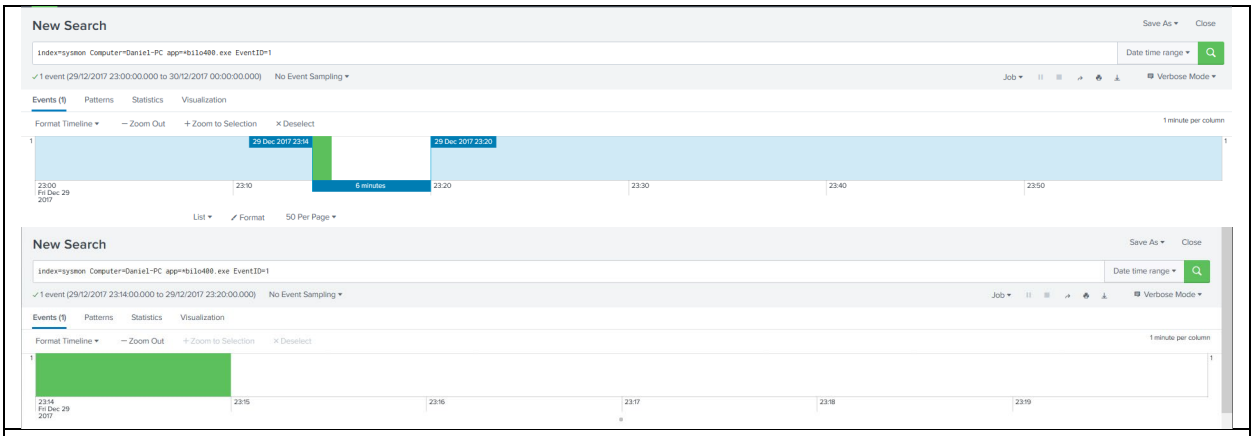
Use the sysmon with the app that's executing the bilo400 and the Event Code 1



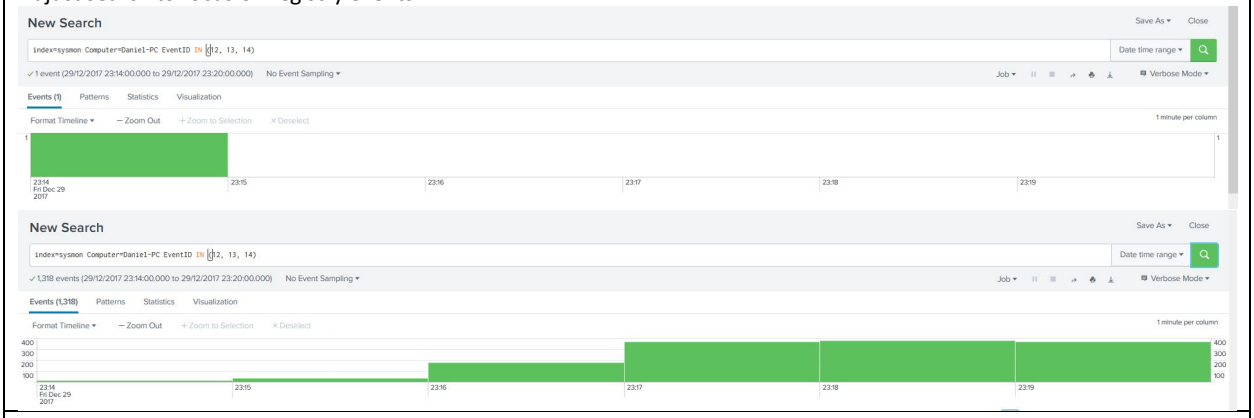
This shows that bilo 400 executed on Daniel-PC at 23:14:33.073 resulting in the device becoming infected with Ramnit Malware

+Zoom into event





Adjust search to focus on registry events.



Now search for modifications you could expect to see for implementation of the Ramnit Malware.

Admin parameter

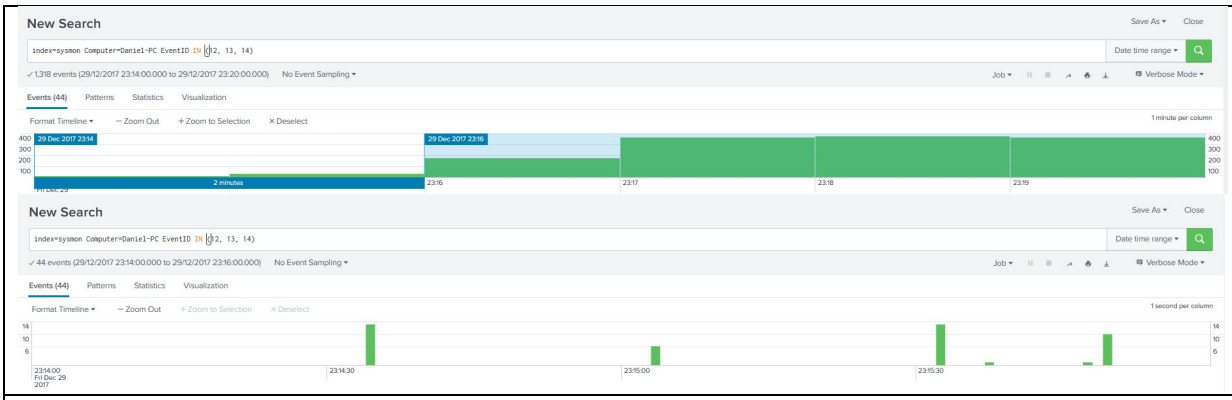
When the “admin” parameter is supplied, the installer creates a mutex as previously described, using 0x14D7 as the seed value. The installer force-exits if it fails to successfully create the mutex.

Then, the installer attempts to lower the computer’s security by modifying the following registry entries and subkeys:

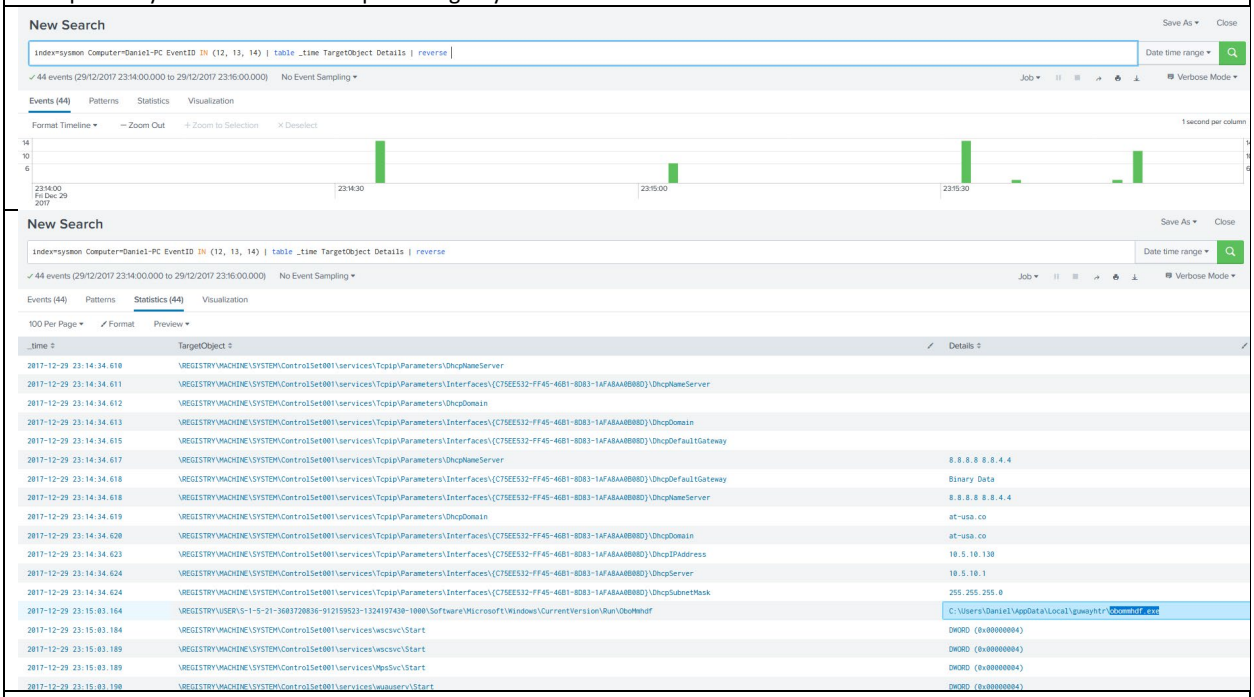
Sets

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\”EnableLUA” = “0”
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center\”FirewallOverride” = “1”
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center\”AntiVirusOverride” = “1”
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center\Svc\”AntiVirusOverride” = “1”
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wscsvc\”Start” = “4”
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\”EnableFirewall” = “0”
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\”DoNotAllowExceptions” = “0”
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\”DisableNotifications” = “1”

Because there are 1,318 events…narrow the search to the first 2 minutes and investigate in smaller time chunks.



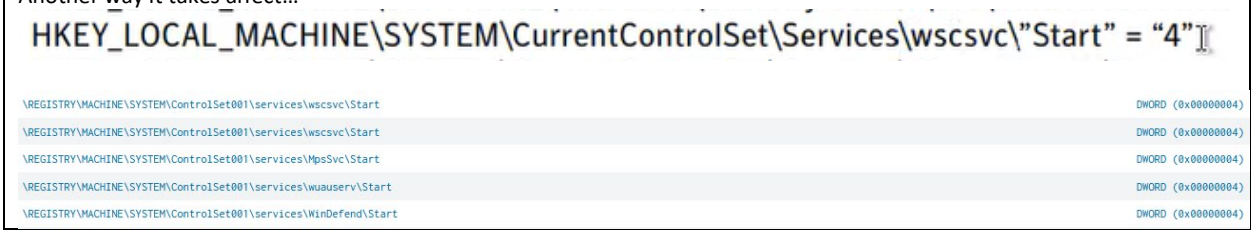
Now profile sysmon to be more helpful in registry fields



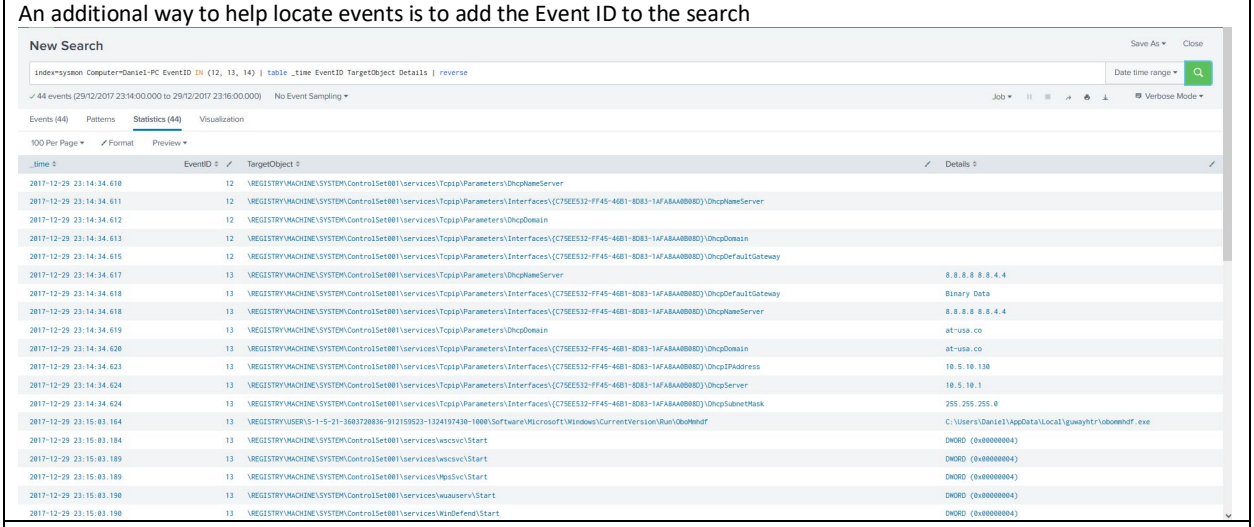
Ramnit does 8 pseudo-random characters

One of the ways Ramnit sets up persistence is it modifies the Run key to ensure a copy of the malware that it made of itself runs at the start.

Another way it takes affect…



An additional way to help locate events is to add the Event ID to the search



You can now see Event 13 listed which is Setting a Value which is evident above.

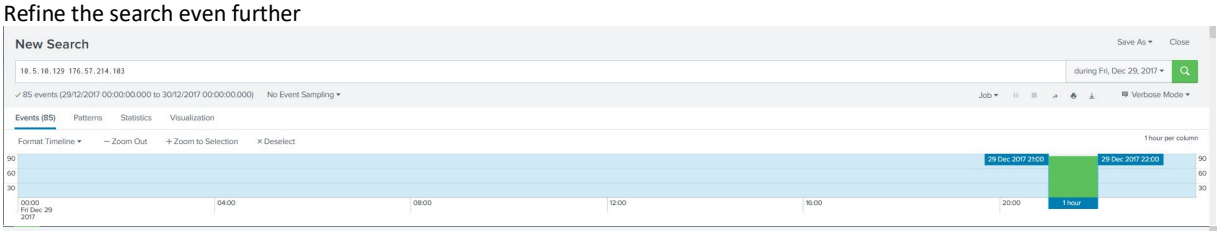
It sets up persistence and then it makes the changes it needs to ensure it will keep running.

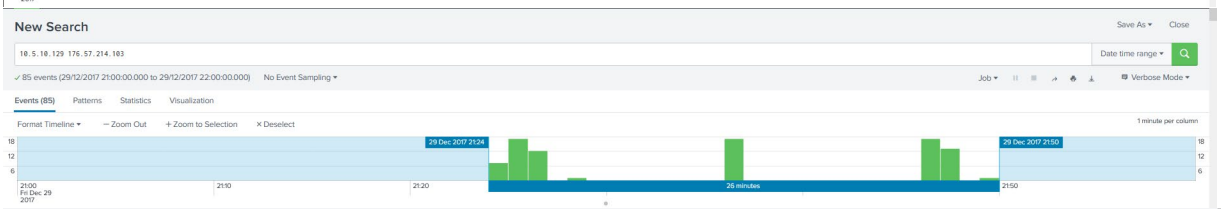
At 23:15:03.164 - .190 registry modifications occurred that decreased the security settings on Daniel-PC.

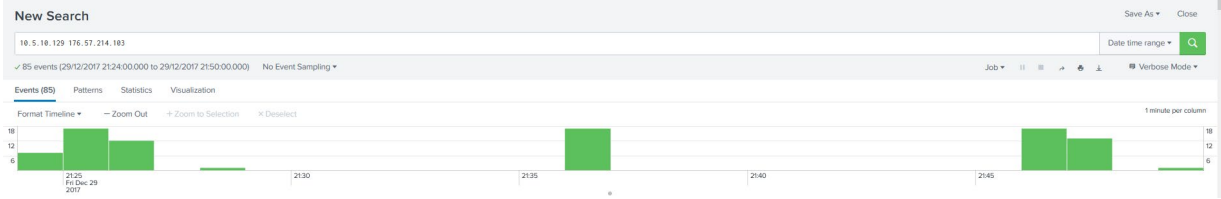
9 - EK COMPROMISE VERIFICATION & MALWARE SUCCESS / FAILURE

Look for all traffic between the compromised device and the EK server

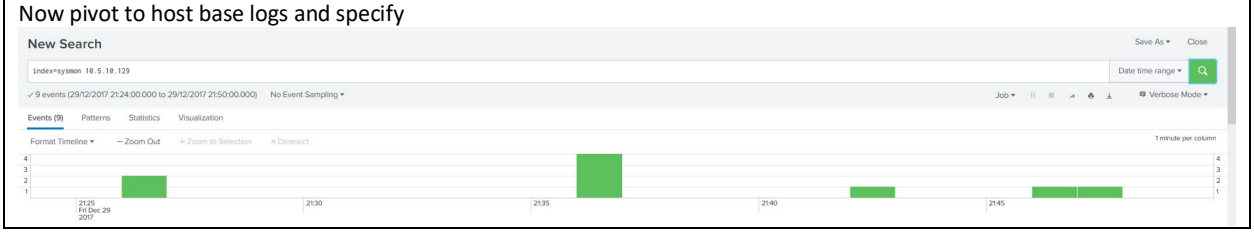
Refine the search even further



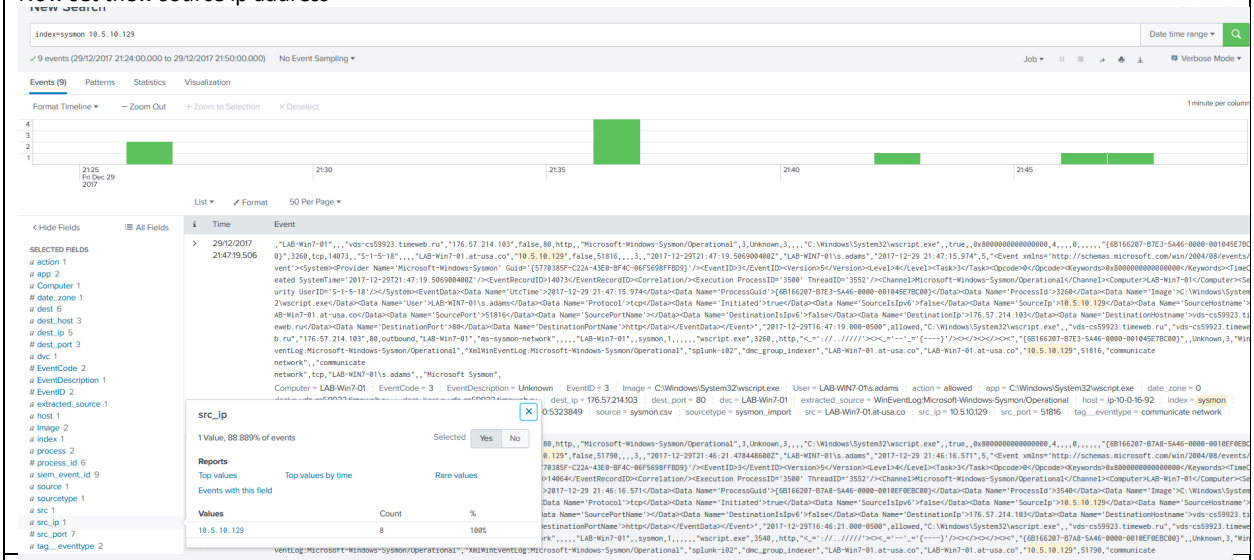


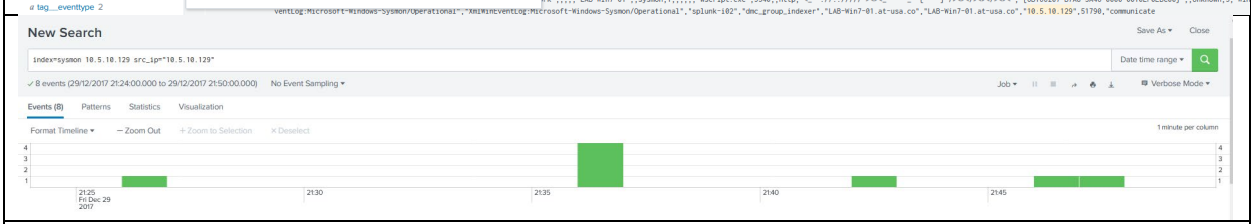


Now pivot to host base logs and specify

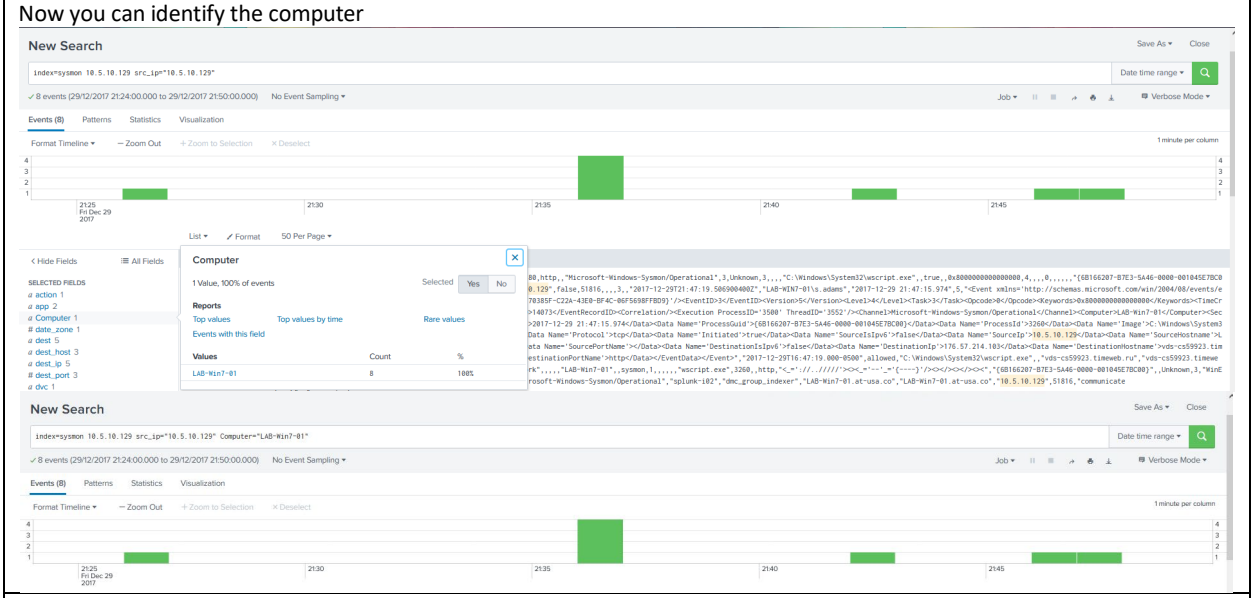


Now set thew source ip address



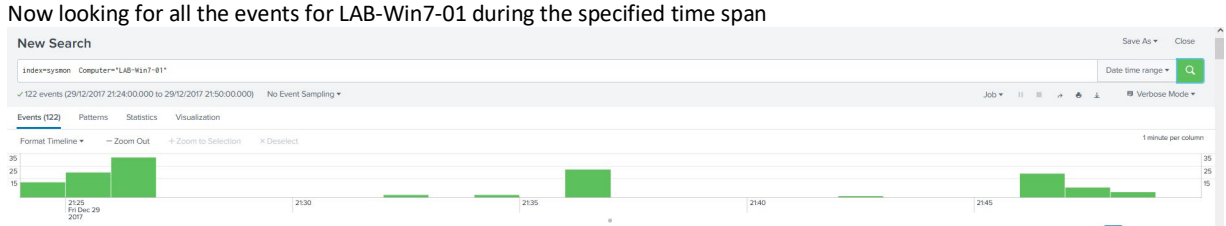


Now you can identify the computer



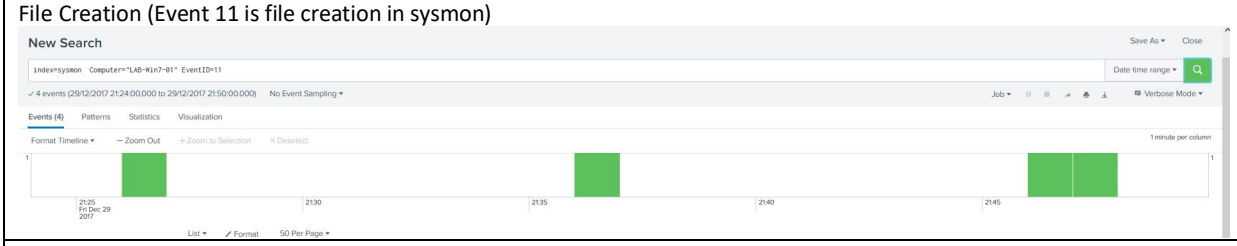
Because I now have the host name I can get rid of the ip address

Now looking for all the events for LAB-Win7-01 during the specified time span



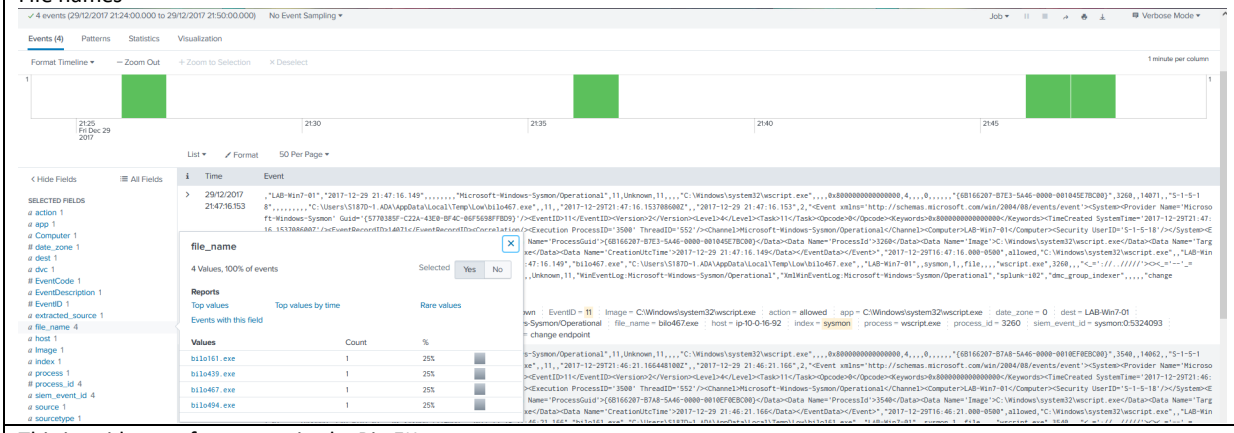
Now looking for the payload delivered…

File Creation (Event 11 is file creation in sysmon)



This search reveals 4 events

File names

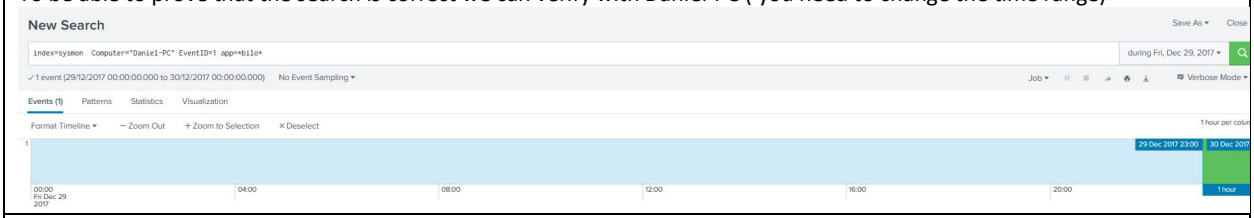


This is evidence of compromise by Rig EK…

Now look for process creation logs by changing from File Creation EventID 11 to Process Creation EventID 1 to see if there is evidence of execution / malware infection.

The search shows no results

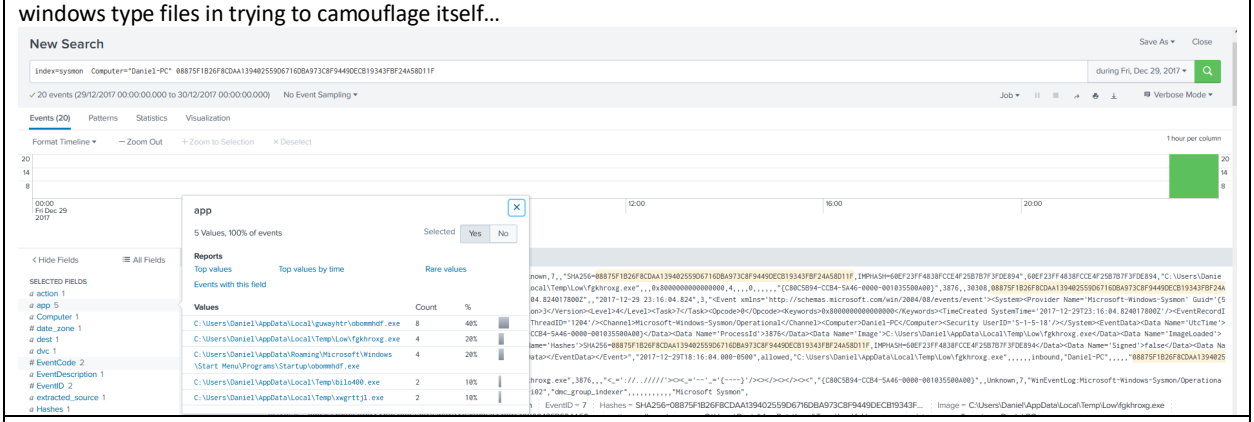
To be able to prove that the search is correct we can verify with Daniel-PC (you need to change the time range)



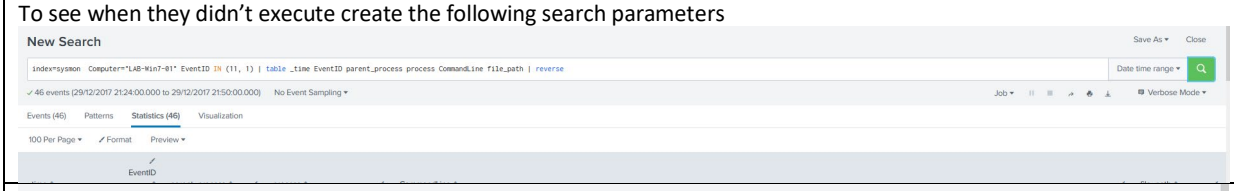
1 process creation event which verifies infection on Daniel-PC, but no process creation events were evident on LAB-Win7-01…verifying that the device was not infected…but payloads were delivered.

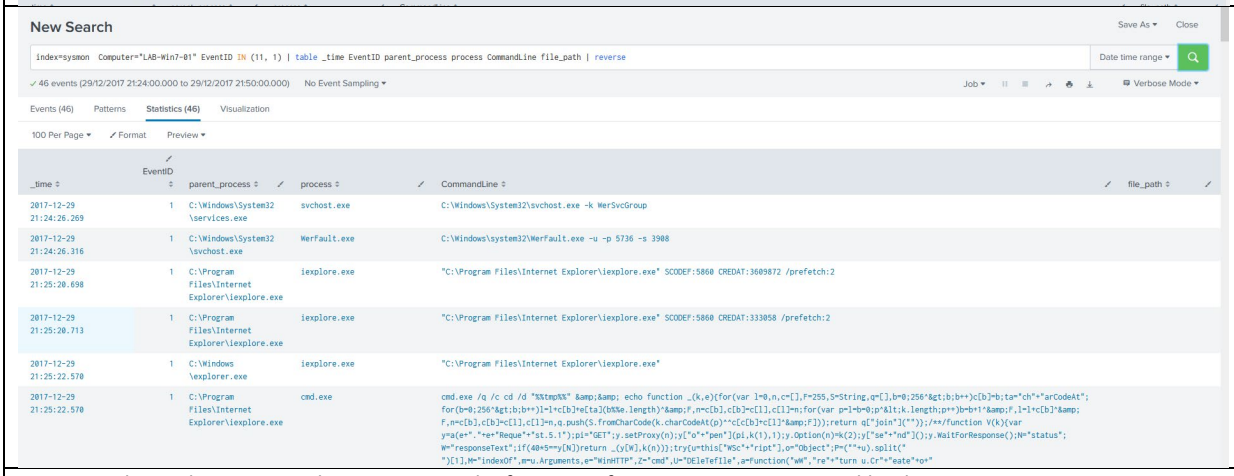
Stepping further…

By using the hash in the search and checking the application field you see multiple 8 random character files…which are windows type files in trying to camouflage itself…

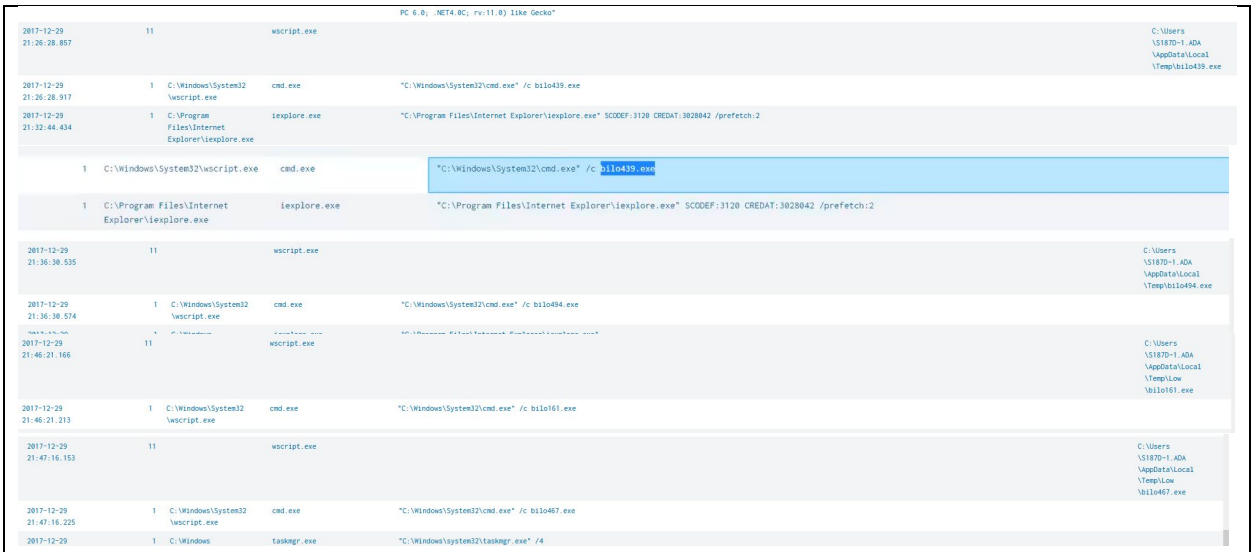


To see when they didn't execute create the following search parameters





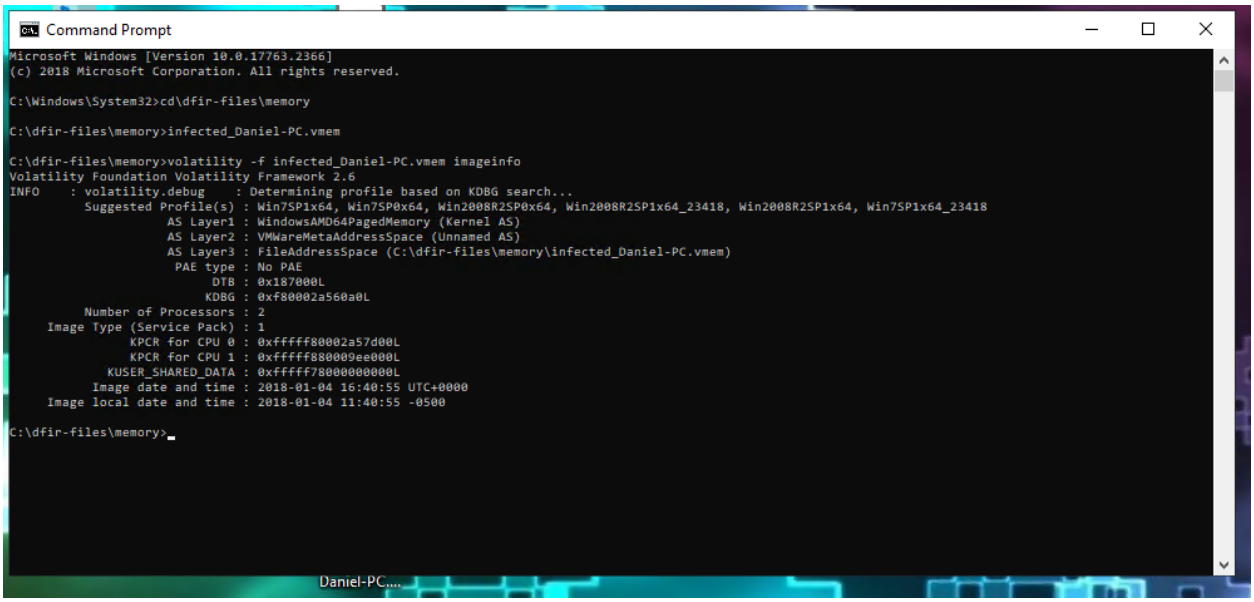
By seeing the Explorer exe cmd exe prompt is the first sign of Win7-01 is compromised by the EK



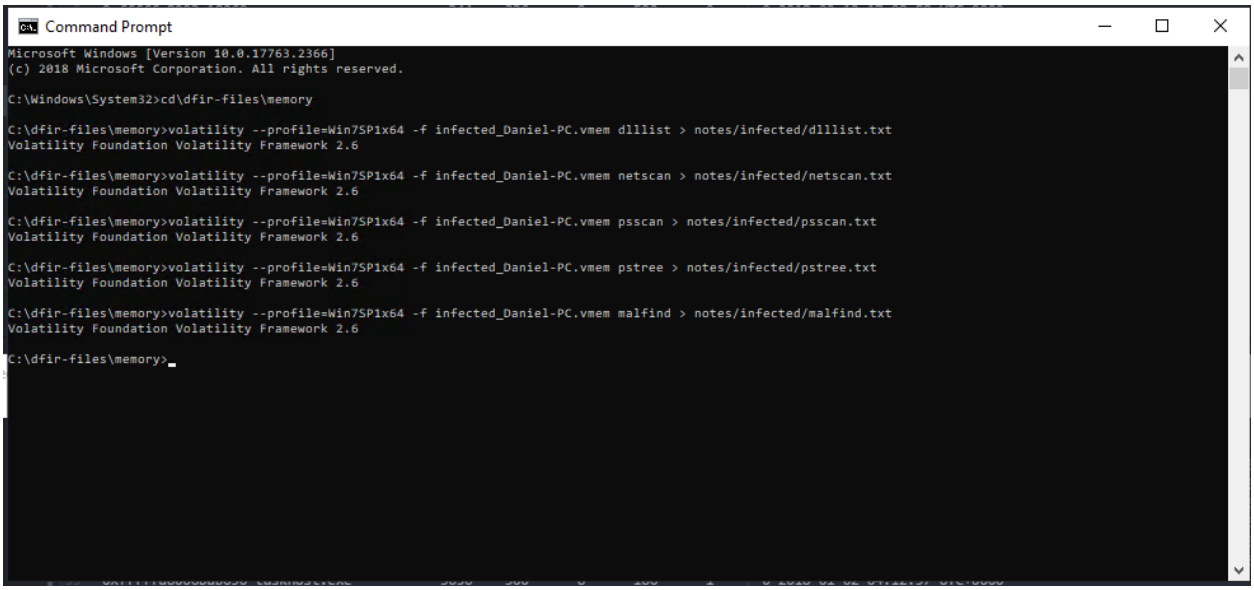
We can see where the 4 bilo payload files tried to execute but you do not see a process creation event which you should see as the next line…below the cmd exe line…it is the same on all 4.

Despite trying to get the process file something did not work.

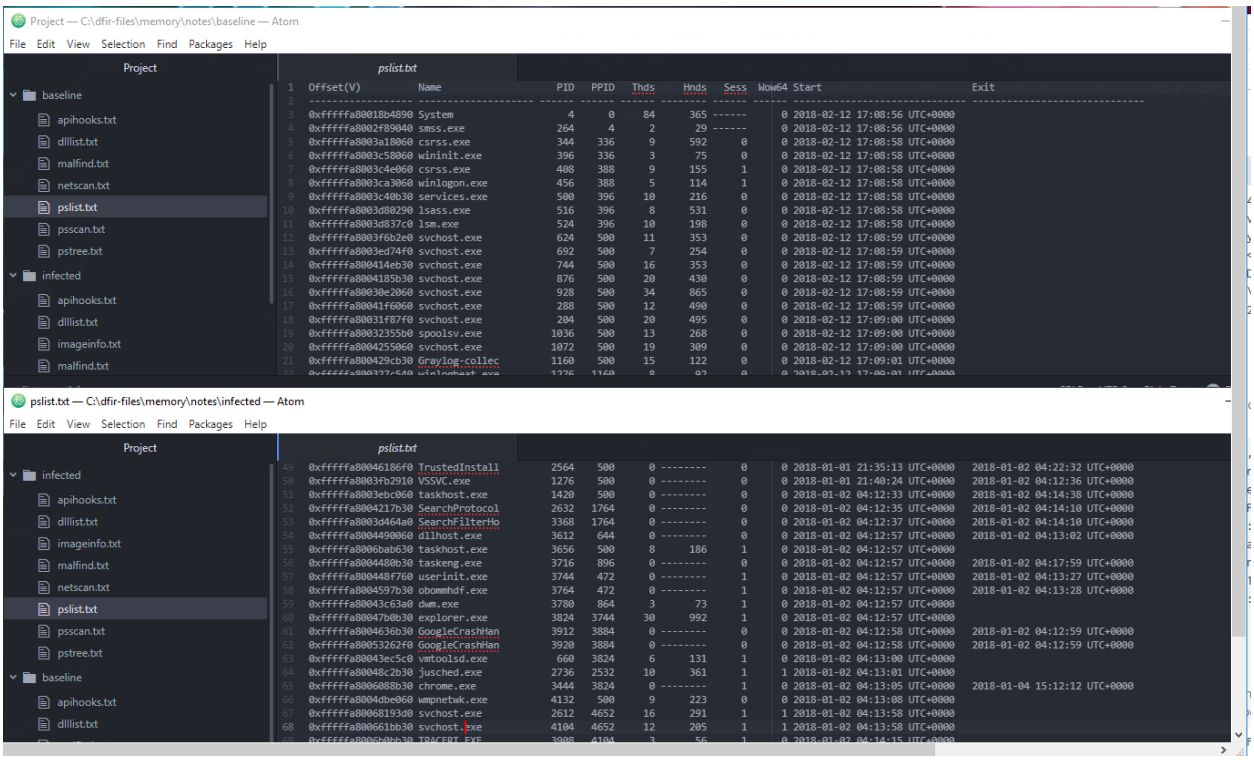
10 – MEMORY



Select various modules for both baseline and infected volatility…



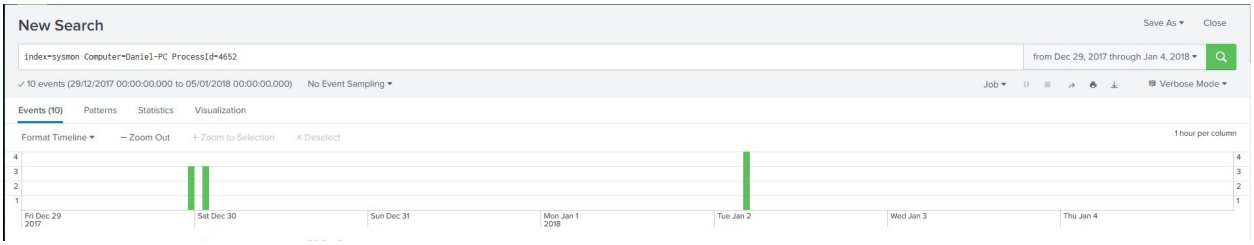
Investigate pslist for both baseline and infected

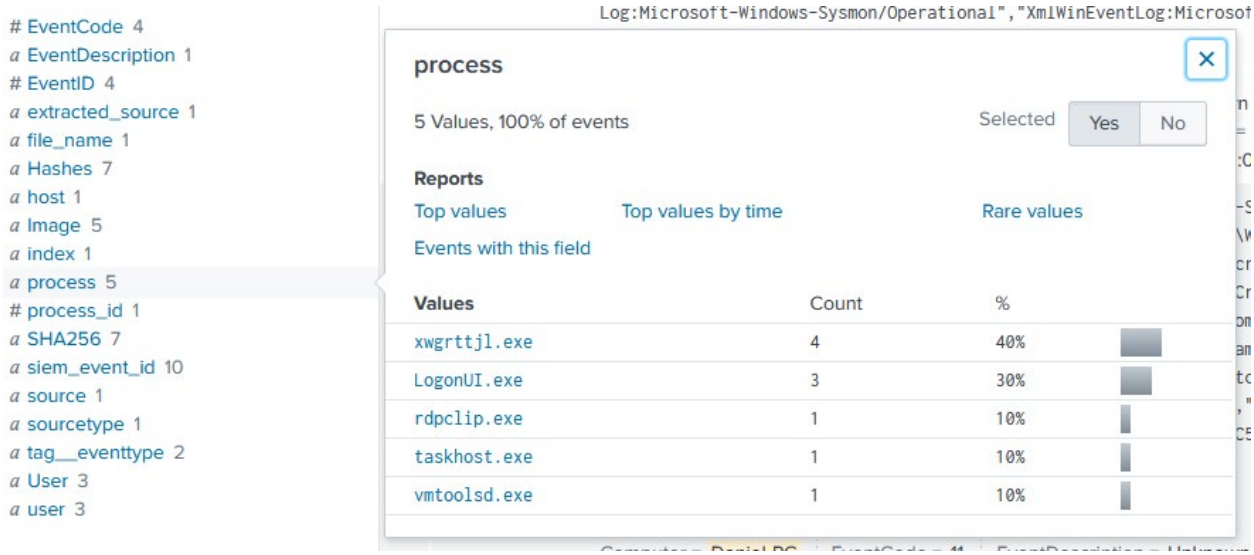


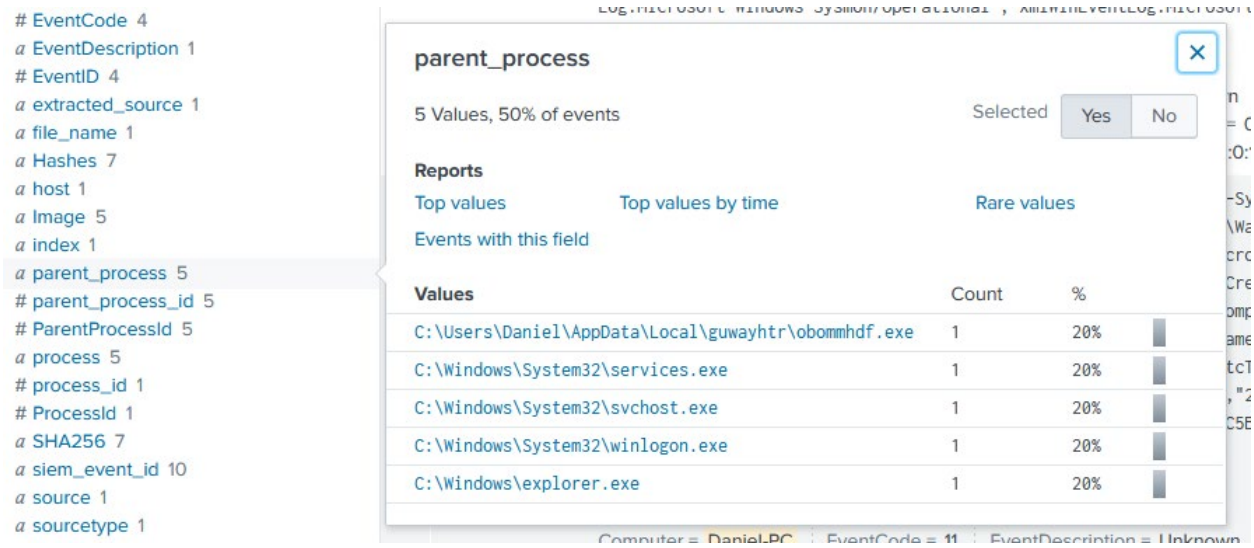
In the infected I can see line 58 which is an anomaly of Ramnit (8-character name) obommhdf.exe

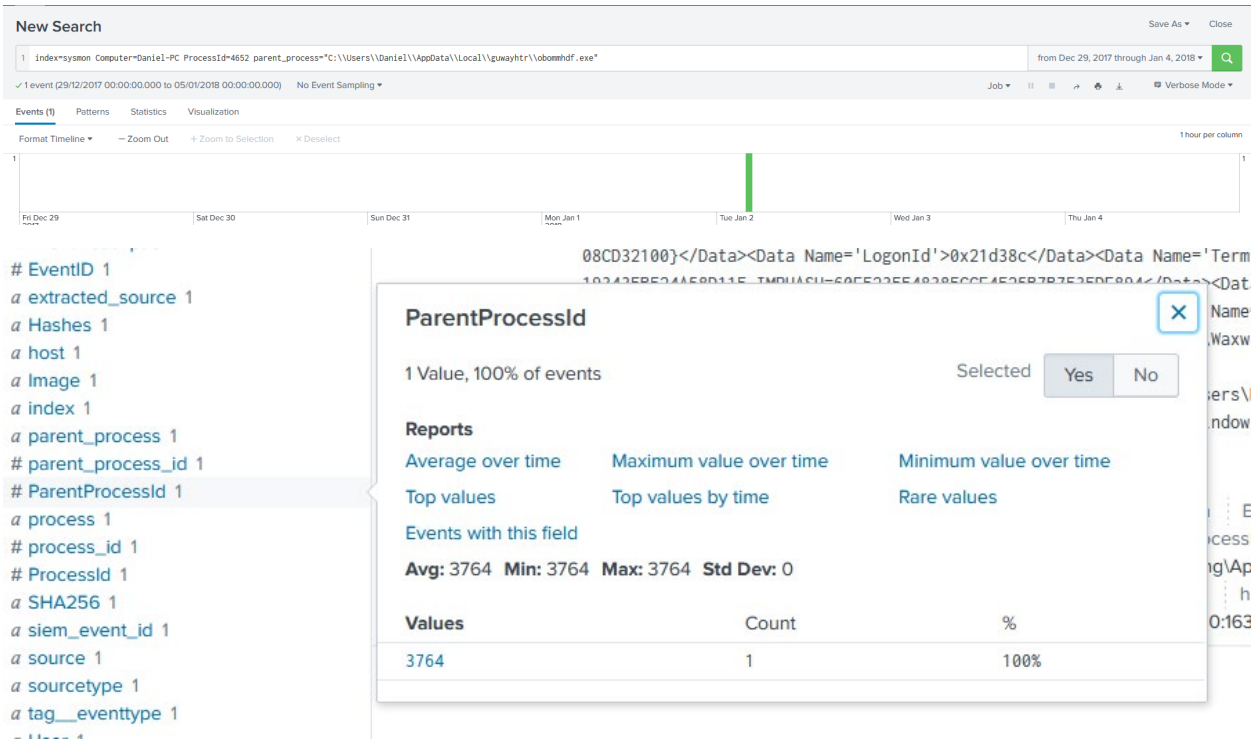
Lines 67 & 68 show svchost.exe with incorrect Parent PID (should only and always be 500, but is 4652) .

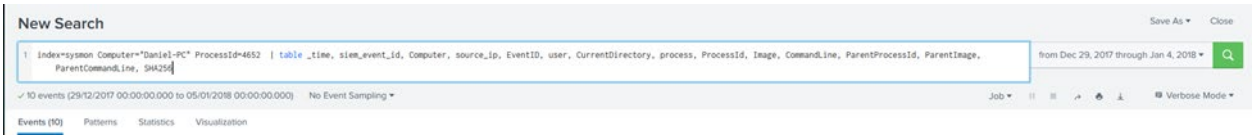
Now investigating on Splunk







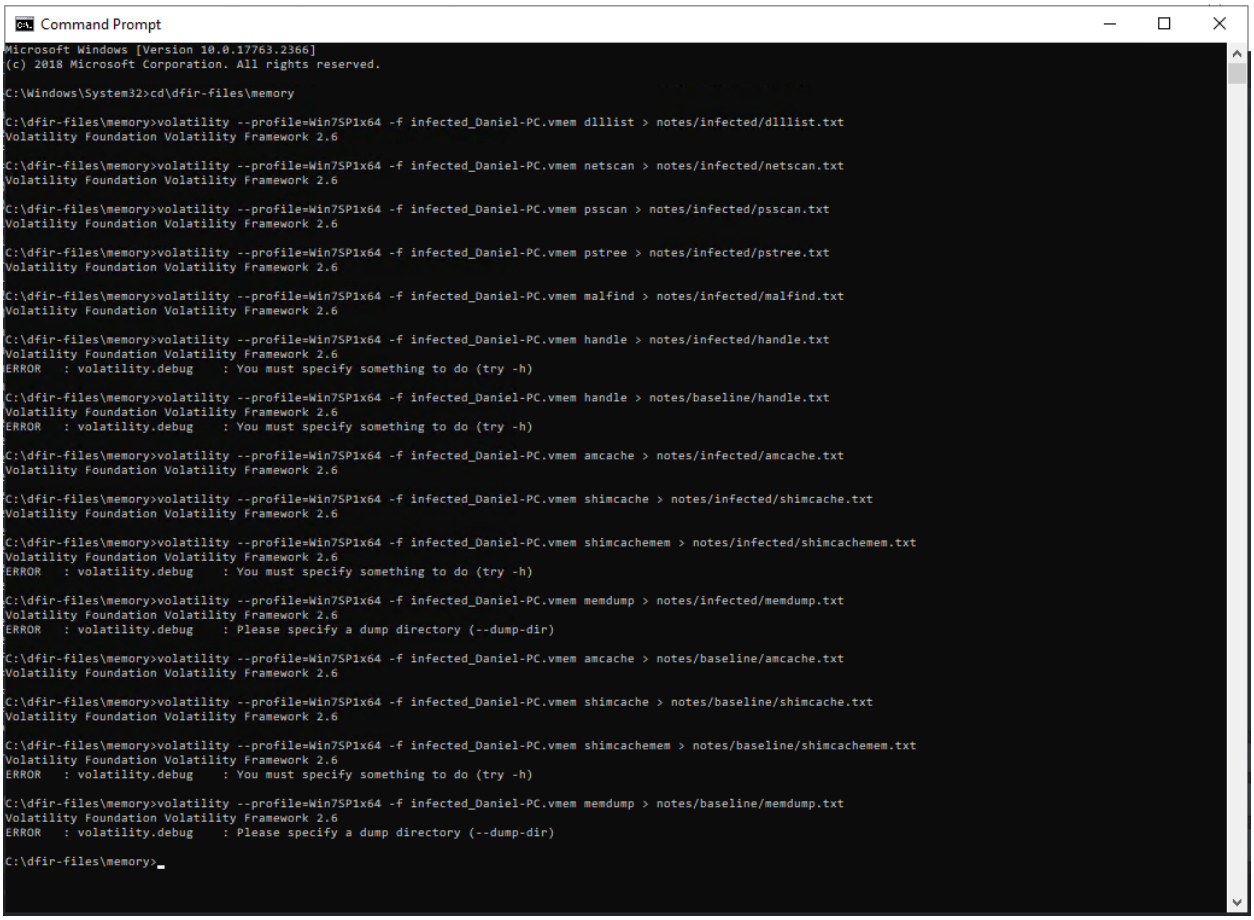




So, by pivoting between our two log sources, we can now reconstruct what happened:

1. obommhdf.exe (PID 3764) spawned a second instance of the 08875f1b... Ramnit executable: xwgrttjl.exe (PID 4652).
2. xwgrttjl.exe (PID 4652) then spawned the two rogue (== without PPID of services.exe (PID 500)!) svchost.exe's: svchost.exe (PID 4104) and svchost.exe (PID 2612).
3. xwgrttjl.exe (PID 4652) then exited the process list, having served its function.
4. obommhdf.exe (PID 3764), svchost.exe (PID 4104) and svchost.exe (PID 2612) remain running.

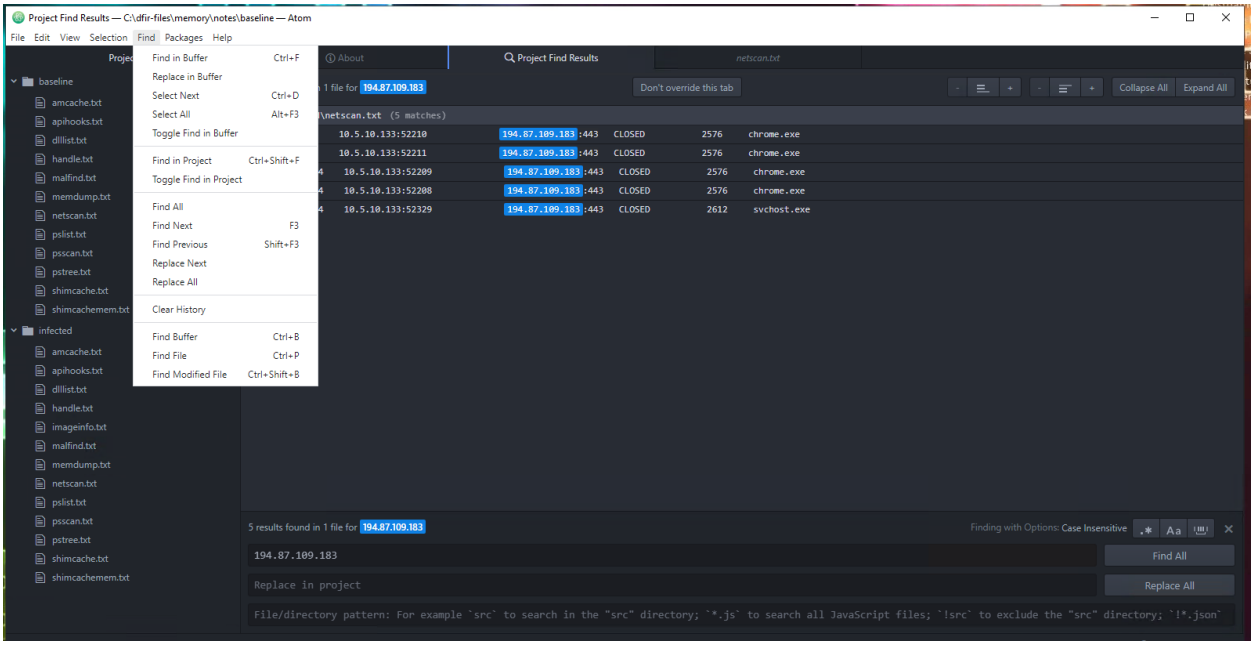
Volatility Command Prompt



To construct the report, you need to bounce back and forth between Atom and Splunk identifying the various processes taking place ie PID & PPID

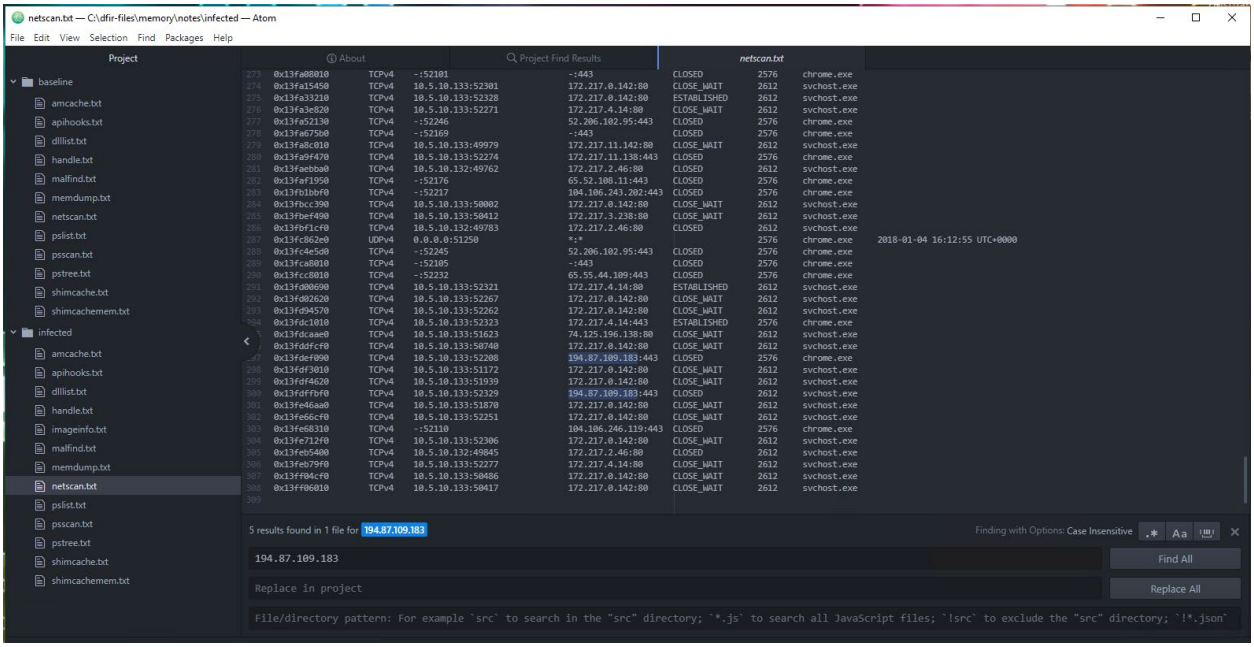
Conduct a search for 194.87.109.183 (known suspect ip address)

Used the Search in Project tab in Find



It returned the above results

Now select any oner of the results



1. Examine the line items and take note of the different identifiers such as: Foreign Address, State, Pid, and Owner.

2. Keep access to the Ramnit white paper available to understand what you're looking at.
3. In the search you see that there are two types of Owner…(chrome.exe and svchost.exe)
    - Research the white paper and find…
        - Purpose: Main installer. Drops device driver and launches it as a service. Injects two Dlls into any newly created process instances of svchost.exe or iexplorer.exe
        - Next, the installer copies itself to %UserProfile%\Application Data\[EIGHT PSEUDO-RANDOM CHARACTERS].exe and attempts to locate the path for svchost.exe and iexplore.exe.

Processes

Table 3 details any processes created during the installation routine and their purpose.

Table 3. Processes created during installation

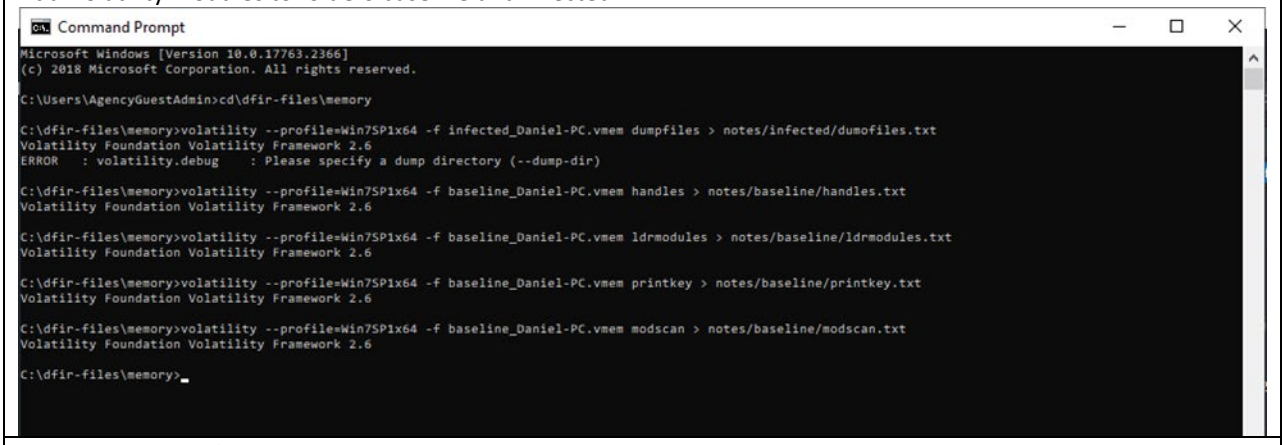
Action	Process	Purpose
Create	svchost.exe or iexplore.exe	Inject DLL_1
Create	svchost.exe or iexplore.exe	Inject DLL_2

        - The DLL_l component acts as a bridge between DLL_2 and a log file. It communicates with DLL_2 using a named pipe to request and receive modules from a remote C&C server. DLL_l is responsible for storing the received modules in an encrypted form in a log file. It also has the ability to load, decrypt, and execute these external modules.

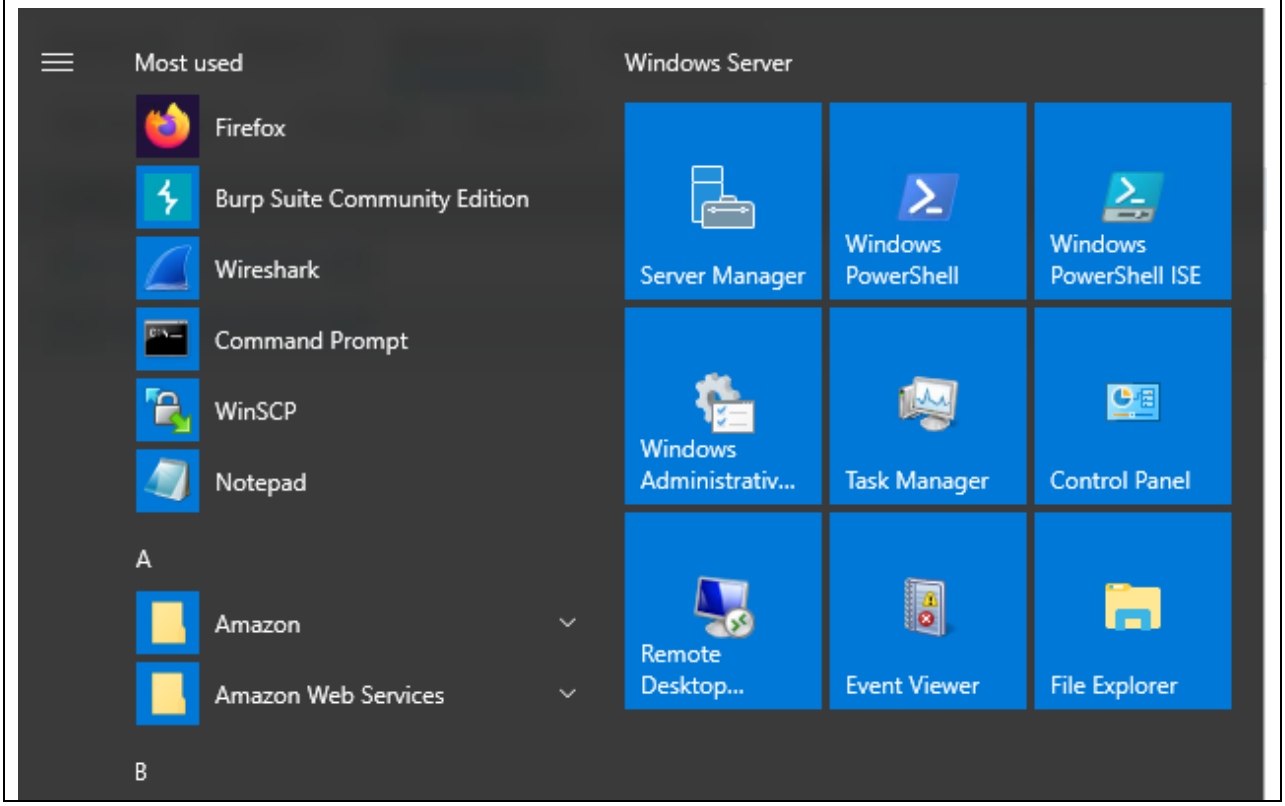
11 – EXECUTION TREE PROCESS

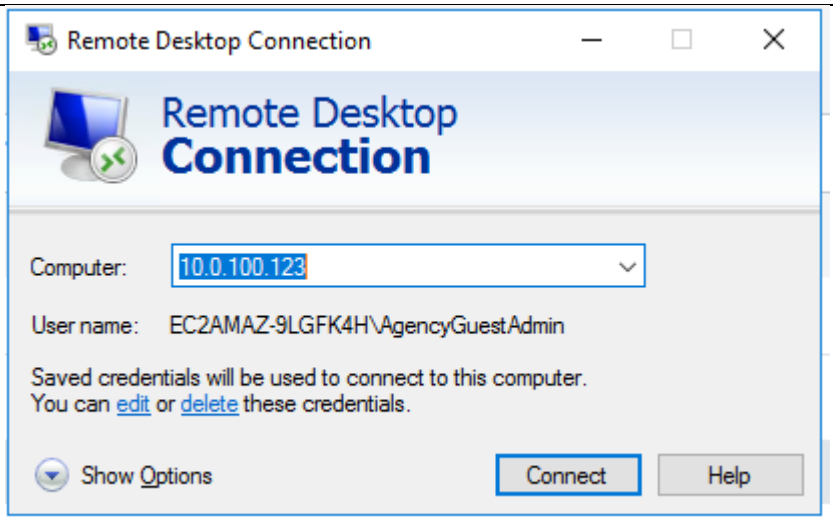
Open command prompt

Add Volatility modules to folders baseline and infected

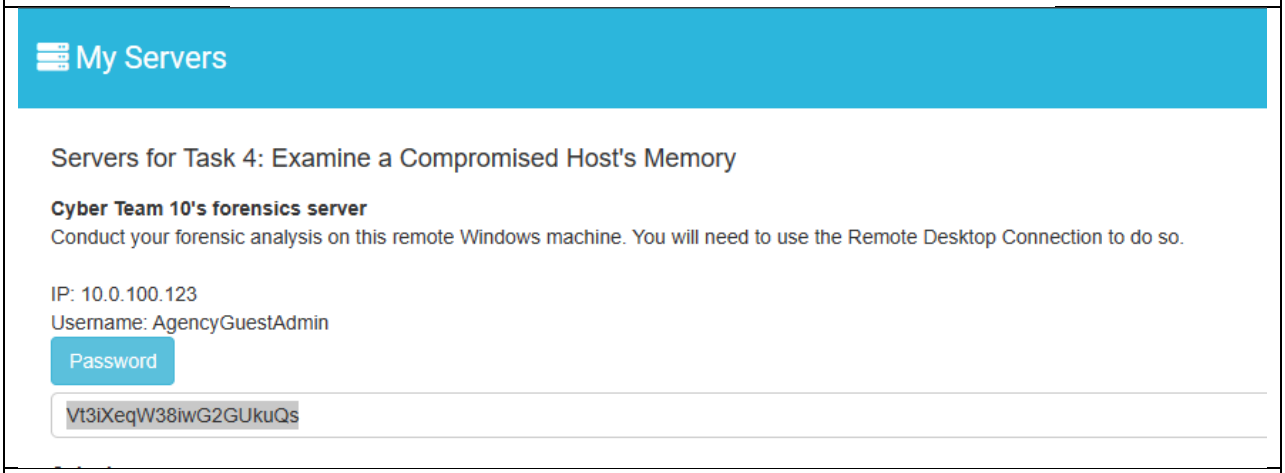


Open Remote Desk Top



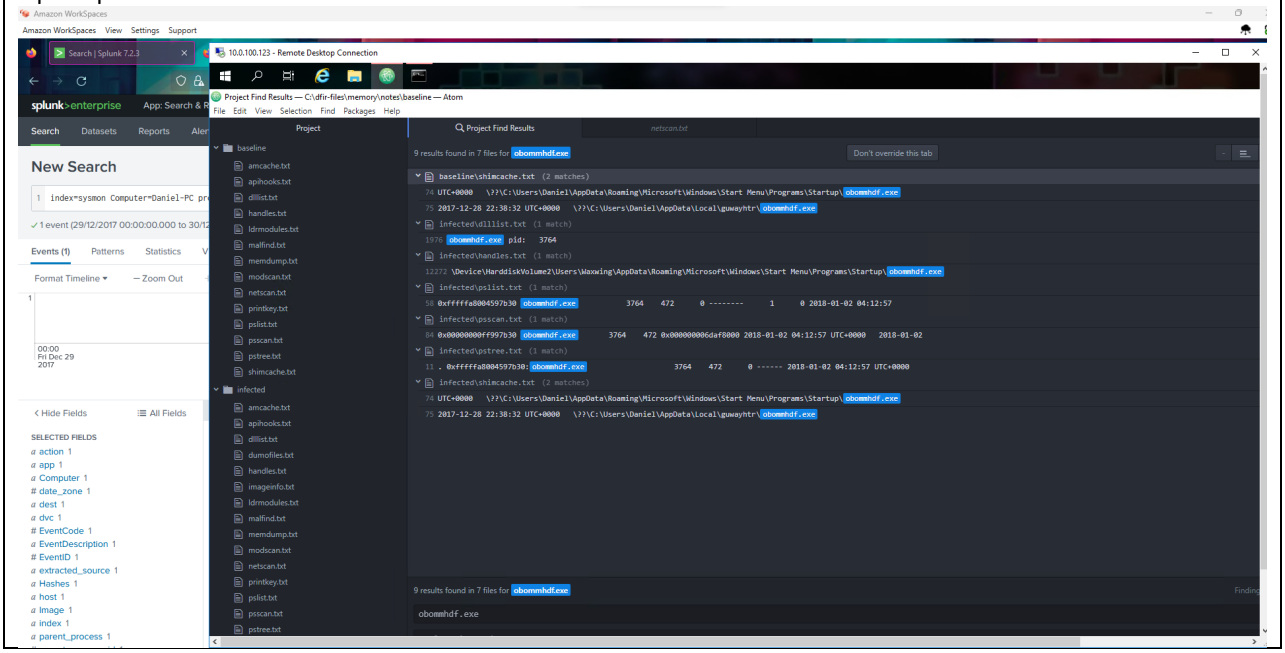


obommhdf.exe



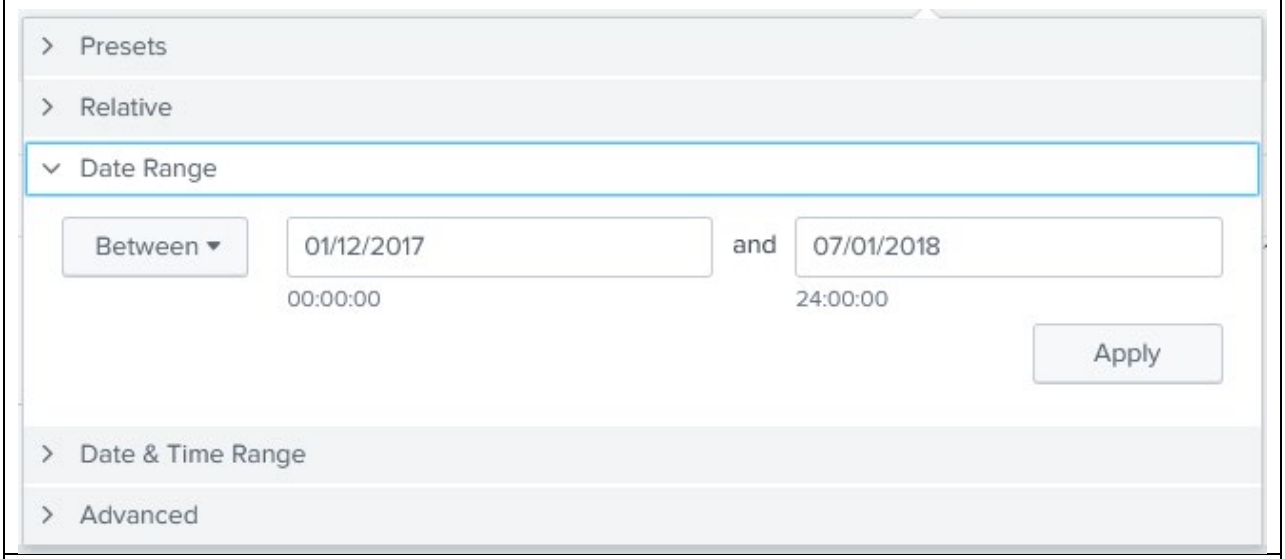
Open Atom

Open Splunk

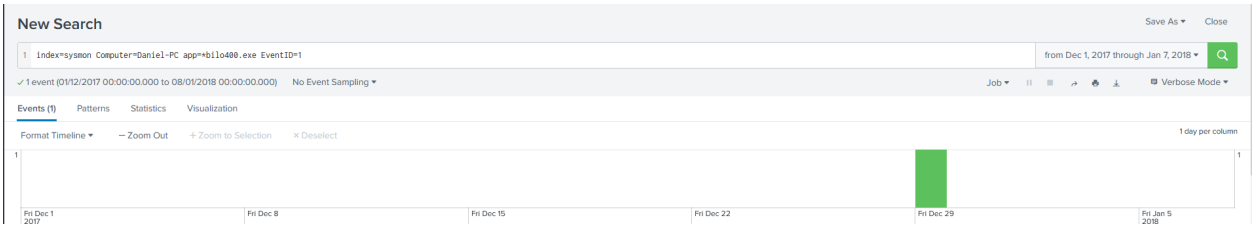


Start point: known event process…bilo400

Set Date range:

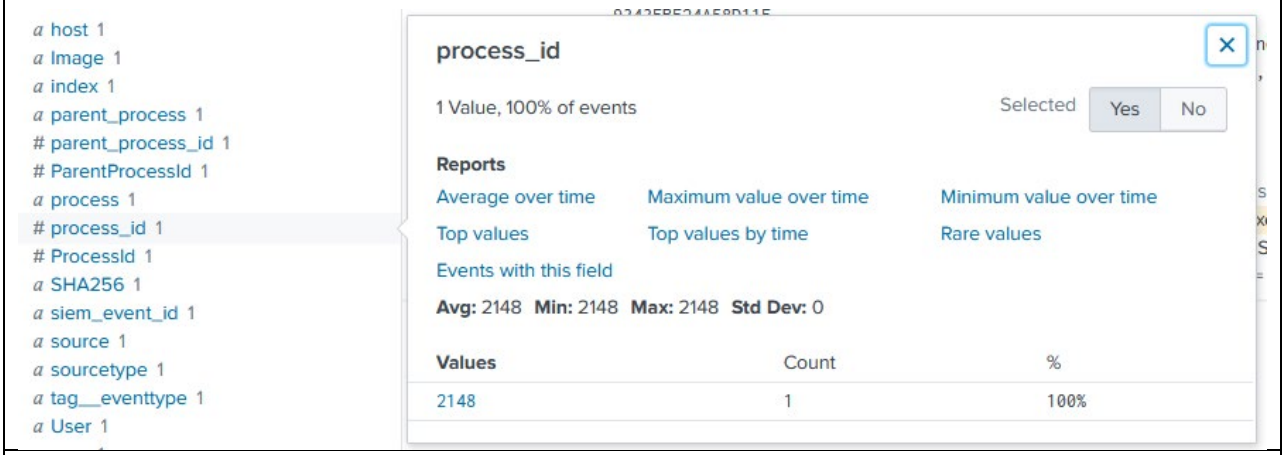


Identify proper Event…in this case start at EventID – 1 Process Creation

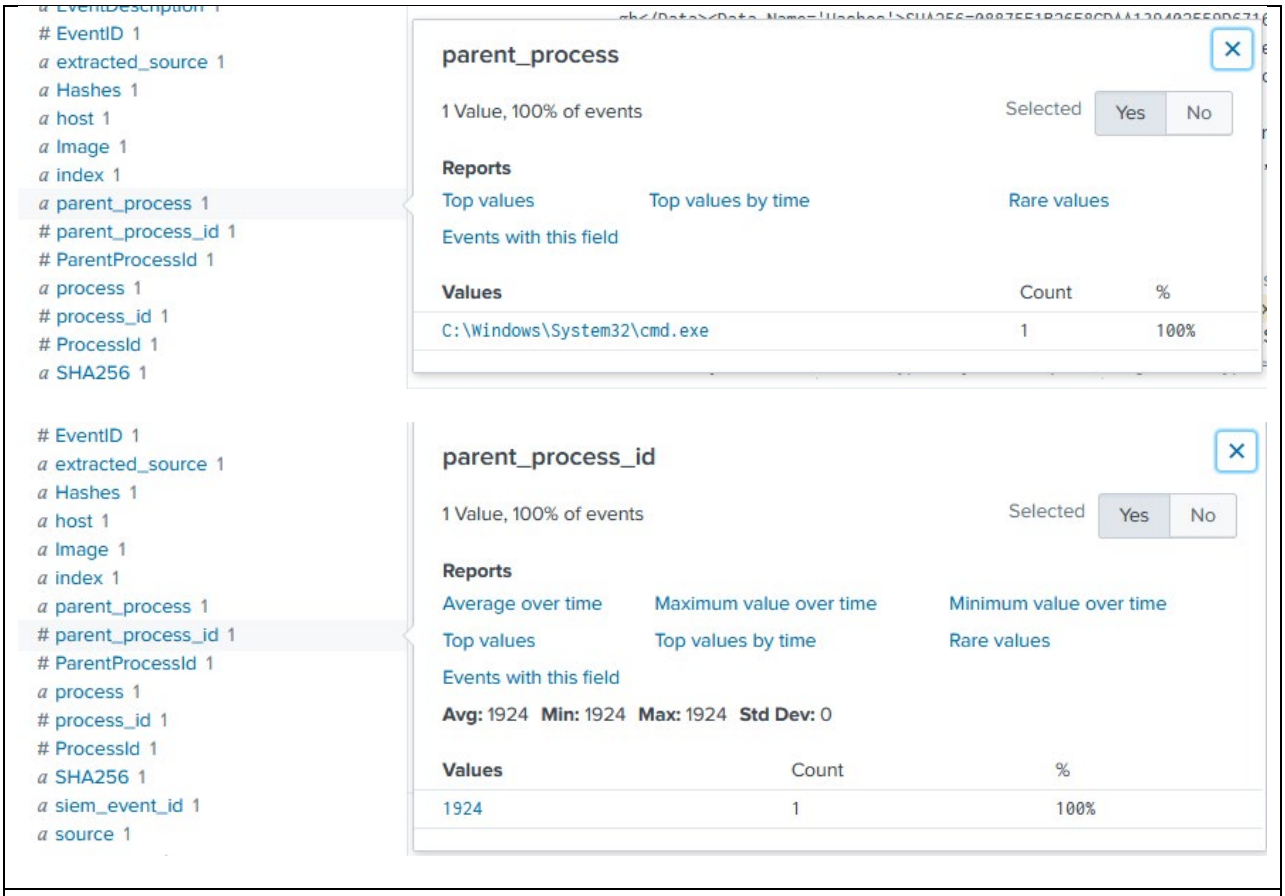


index=sysmon Computer=Daniel-PC app=*bilo400.exe EventID=1

Identify Process Identification Number



What created bilo400 - Identify Parent Process and Parent Process ID

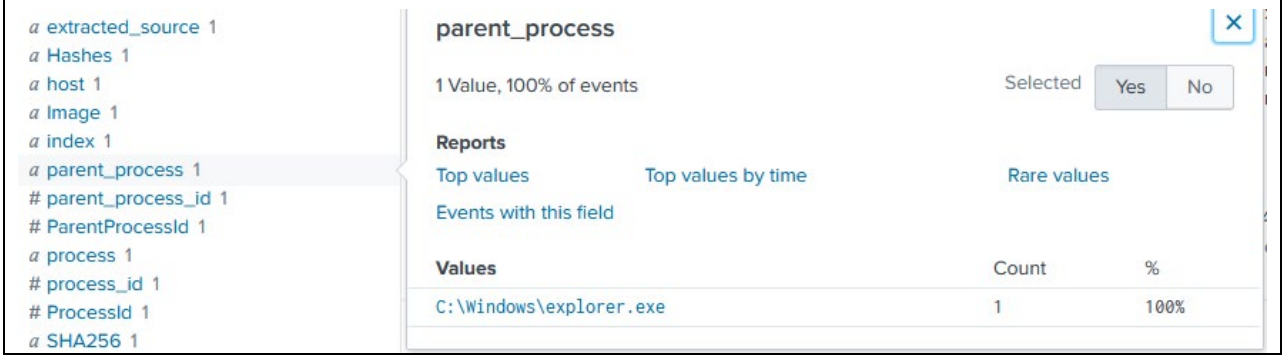


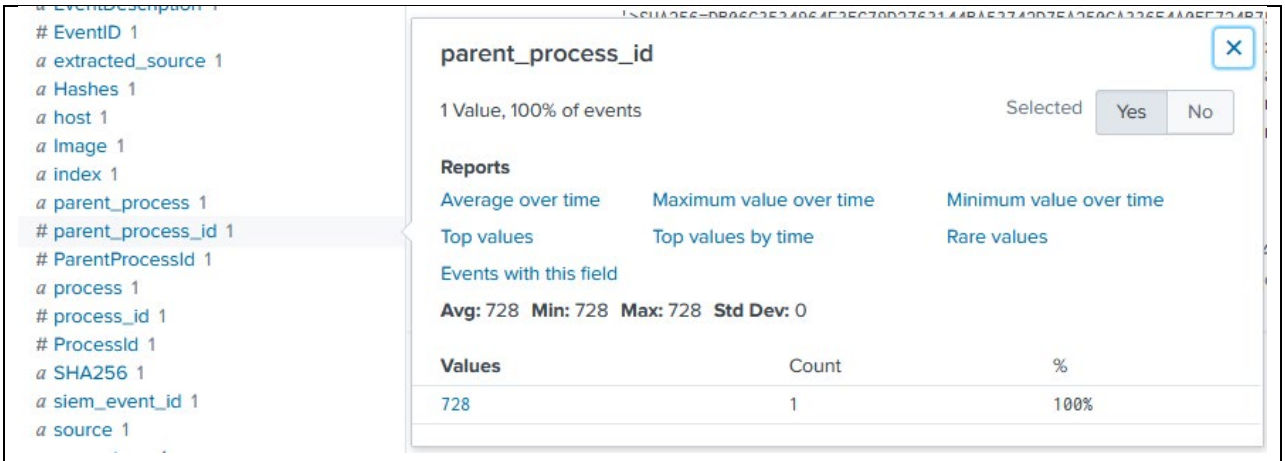
What created cmd.exe PID 1924

To continue backwards….repeat process as above…

What created cmd.exe - Identify Parent Process and Parent Process ID

index=sysmon Computer=Daniel-PC process=*cmd.exe process_id=1924

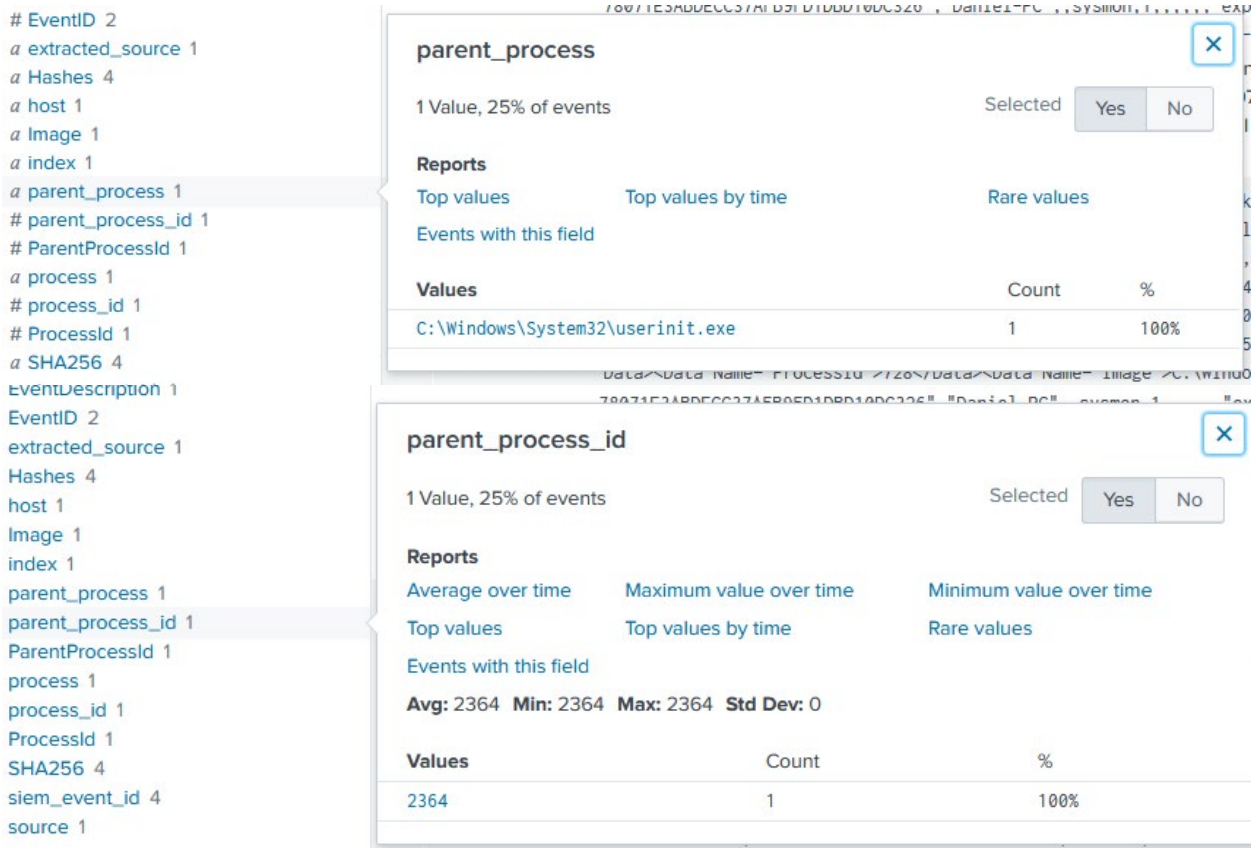




To continue backwards….repeat process as above…

What created explorer.exe - Identify Parent Process and Parent Process ID

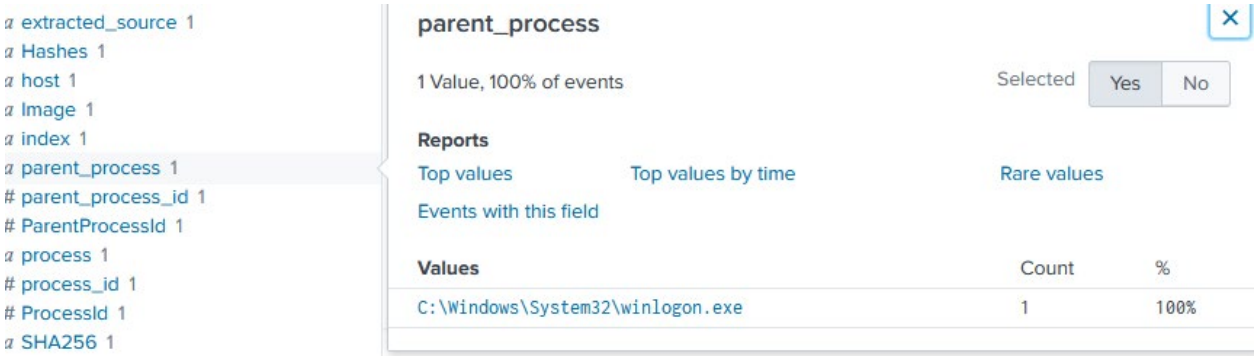
index=sysmon Computer=Daniel-PC process=*explorer.exe process_id=728



To continue backwards….continue to repeat process as above…until you've reach the stopping point or beginning…

What created explorer.exe - Identify Parent Process and Parent Process ID

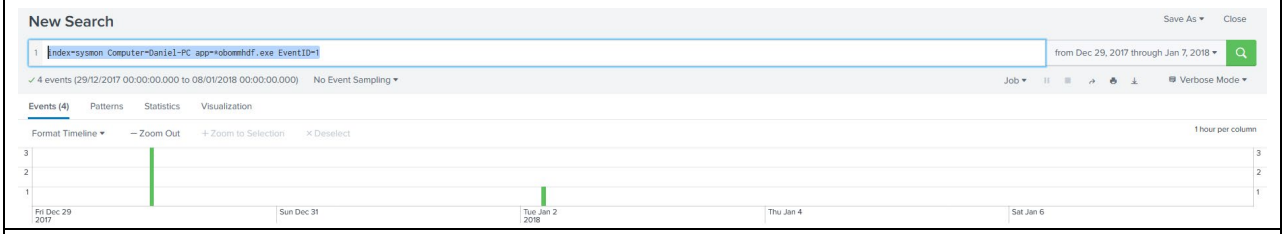
index=sysmon Computer=Daniel-PC process=*userinit.exe process_id=2364



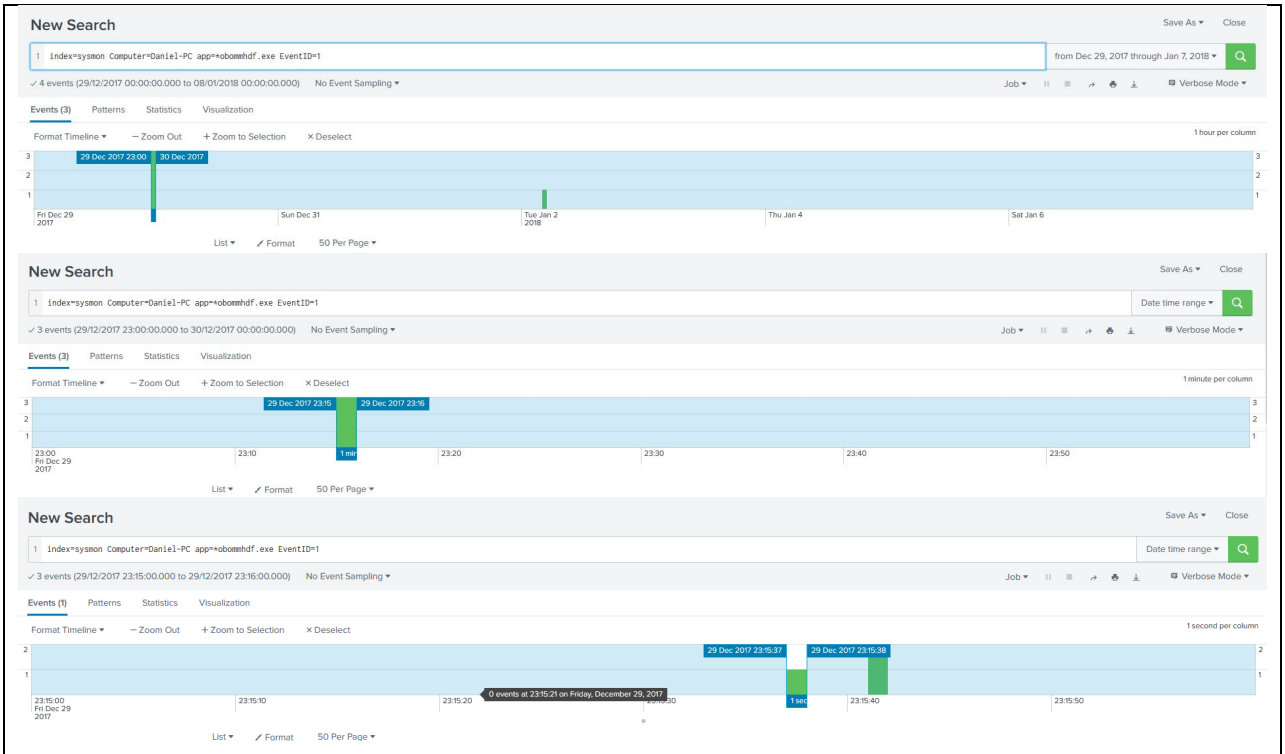
To continue forward to discover what happens next: example obommhdf as start point

Set correct timeline
Search correct Event

index=sysmon Computer=Daniel-PC app=*obommhdf.exe EventID=1

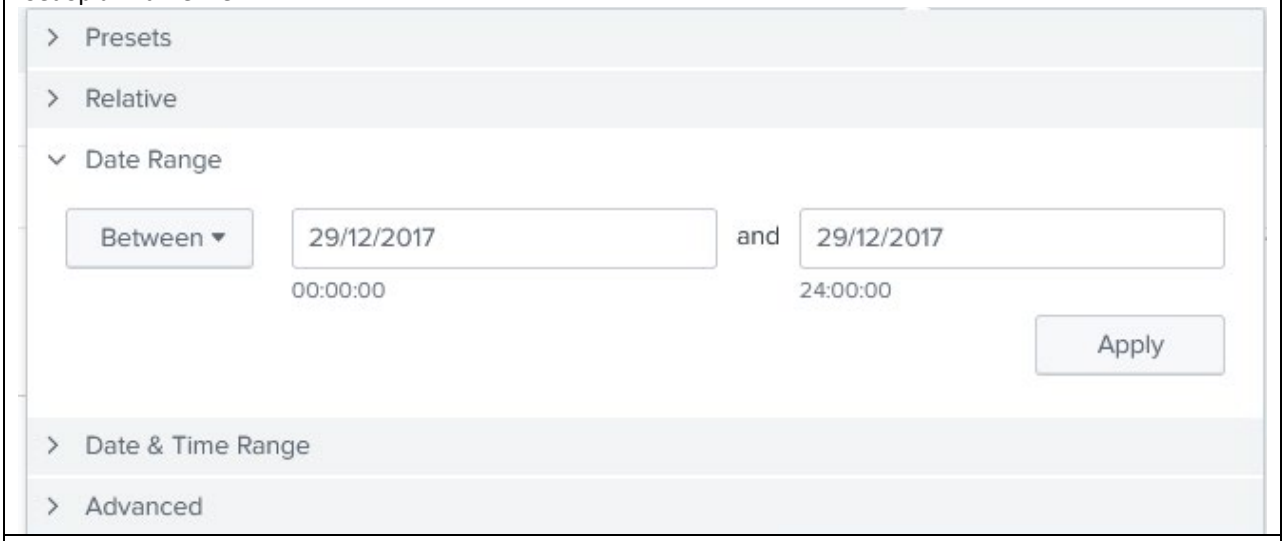


Zero in on (for this example the first instance) by zooming in to single event

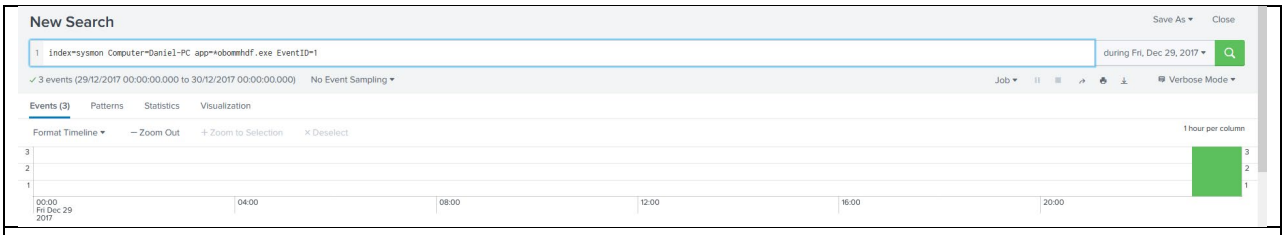


As before in the earlier steps discover what created each step working backwards…
To continue working forward to determine what happened after the event.

Set Splunk timeline

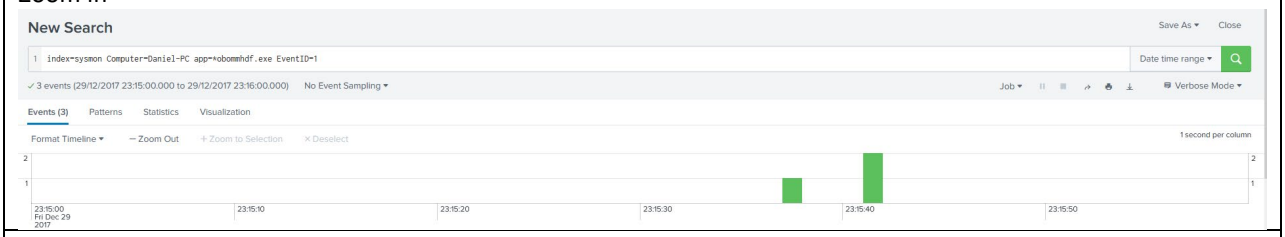


Will work with the first obommhfd.exe first

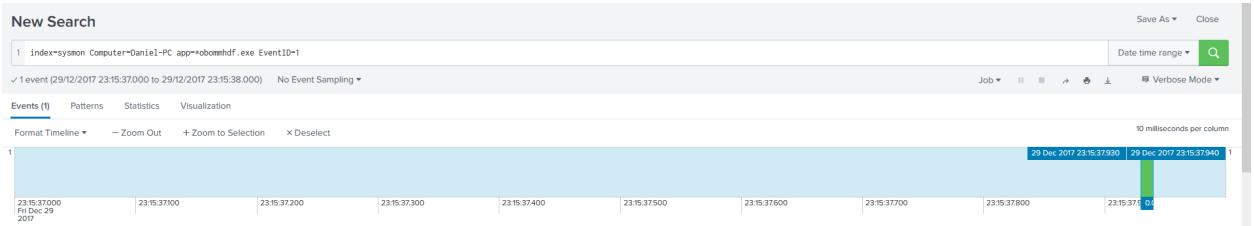


Zoom in

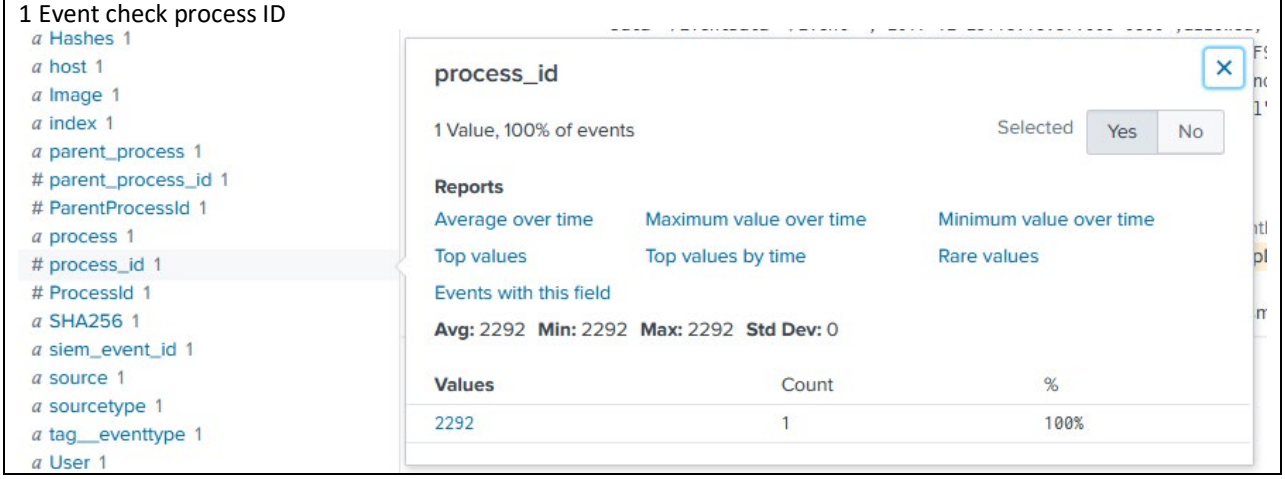
Zoom in



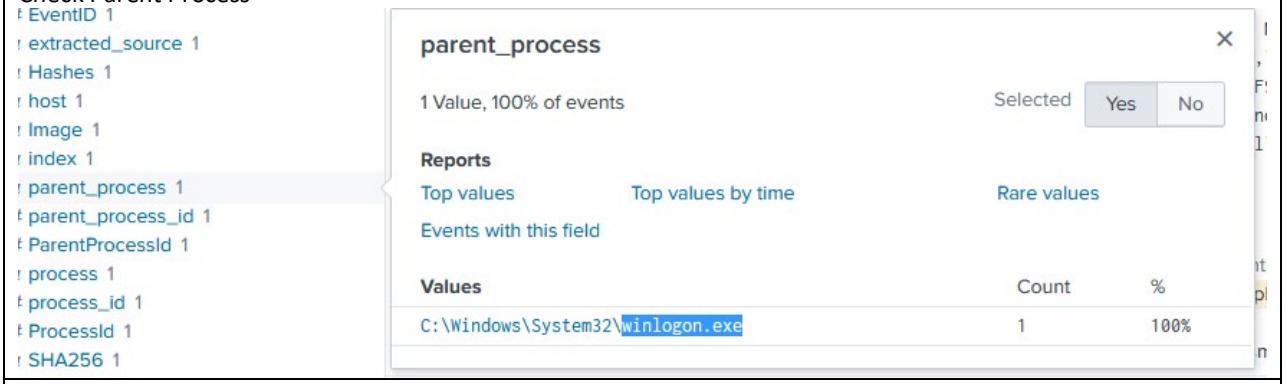
Zoom in



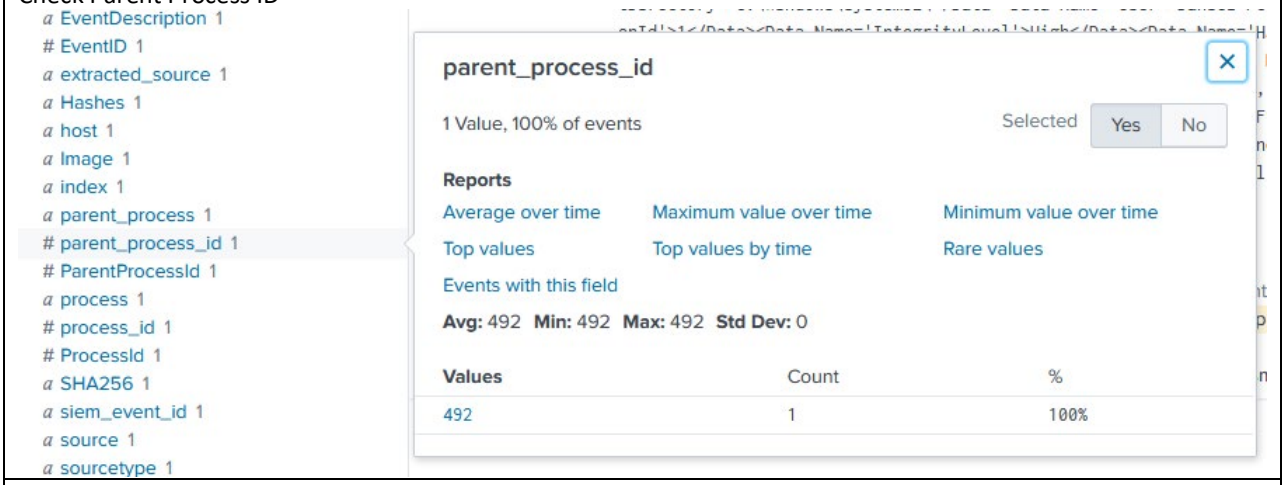
1 Event check process ID



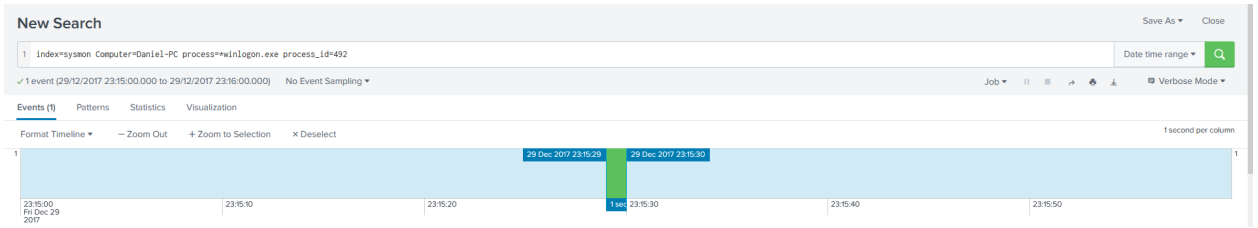
Check Parent Process



Check Parent Process ID

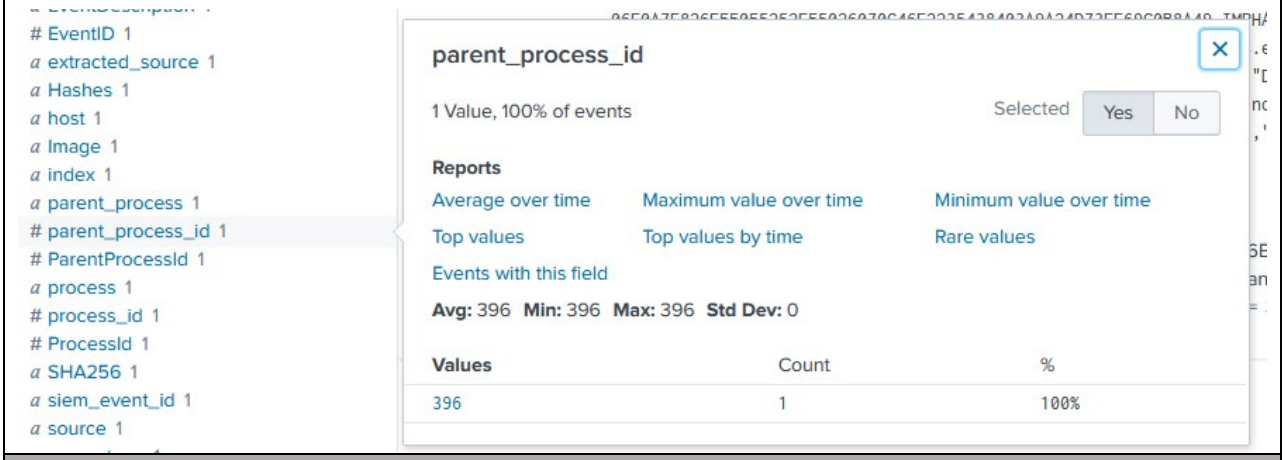


Winlogon is as far as is needed but If you wanted to continue back…
Edit search to winlogon and process 492



Check Parent Process

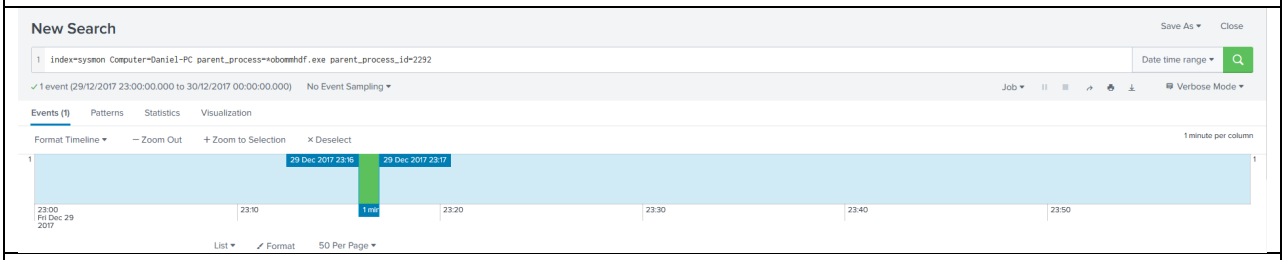
Check Parent Process ID



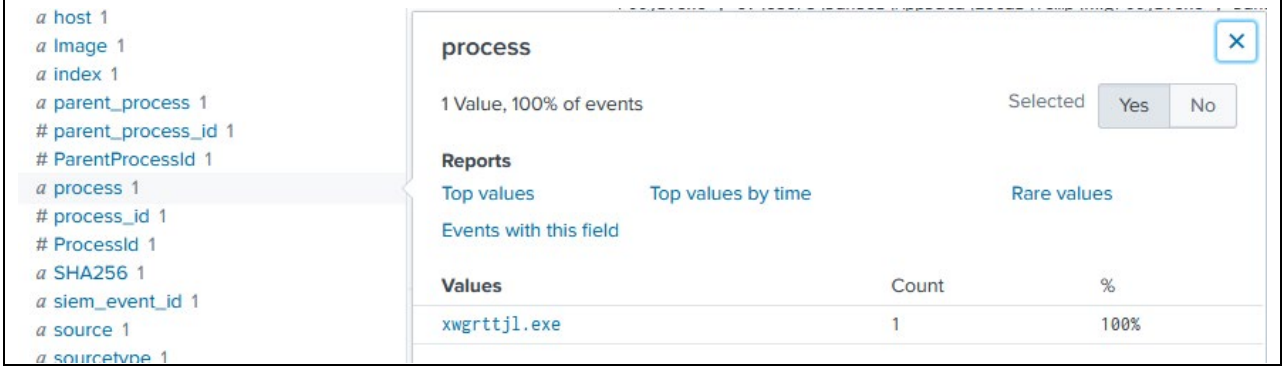
Continue all the way back system at a later time for interest…as per the above steps

Now move forward with obommhdf.exe to see if it created any children…shift the search from app= to parent process

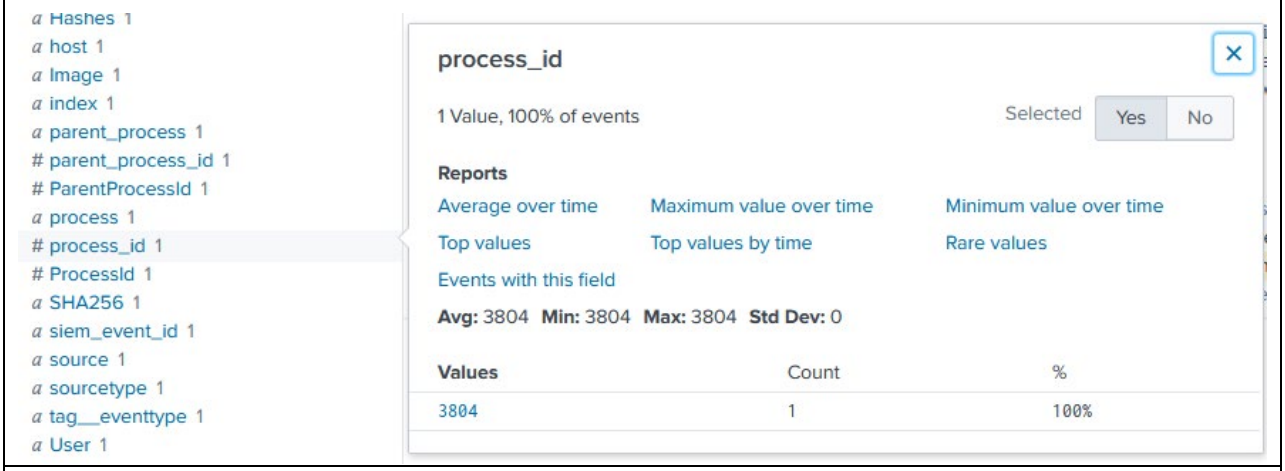
Be sure to zoom out enough to open the timeline.



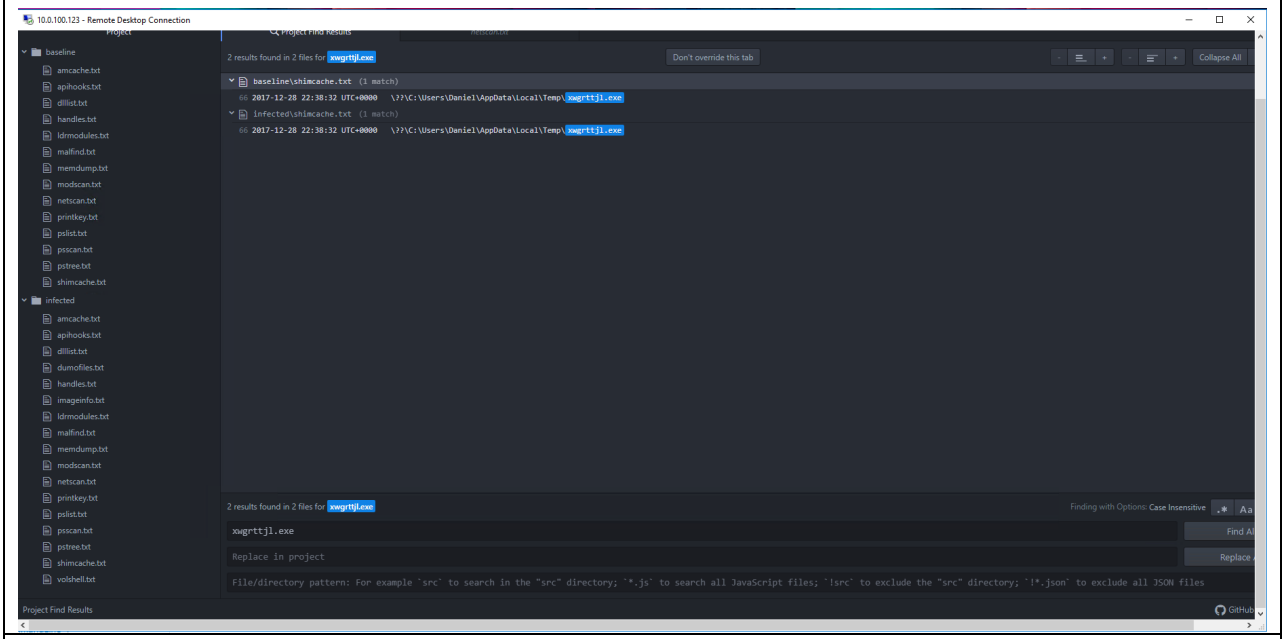
Check the process



Check Process ID

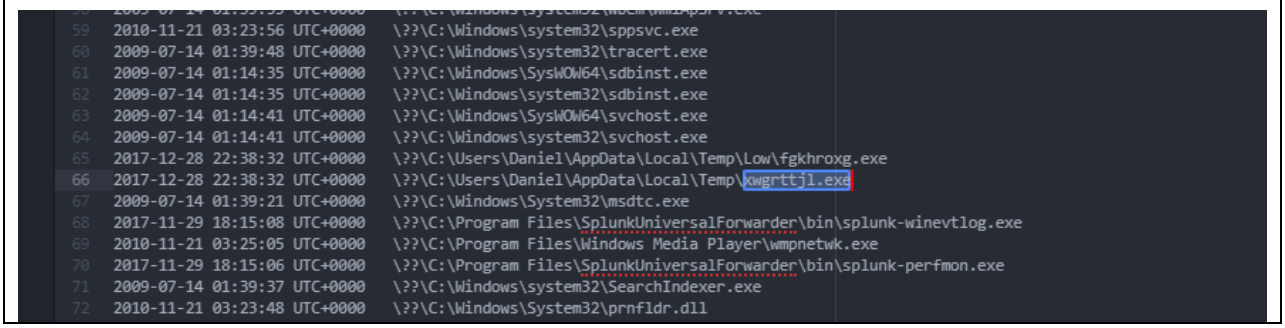


Now copy xwgrttjl.exe and go into Atom and search project



Shows up in new module shimcache

Click onto line item and it opens up

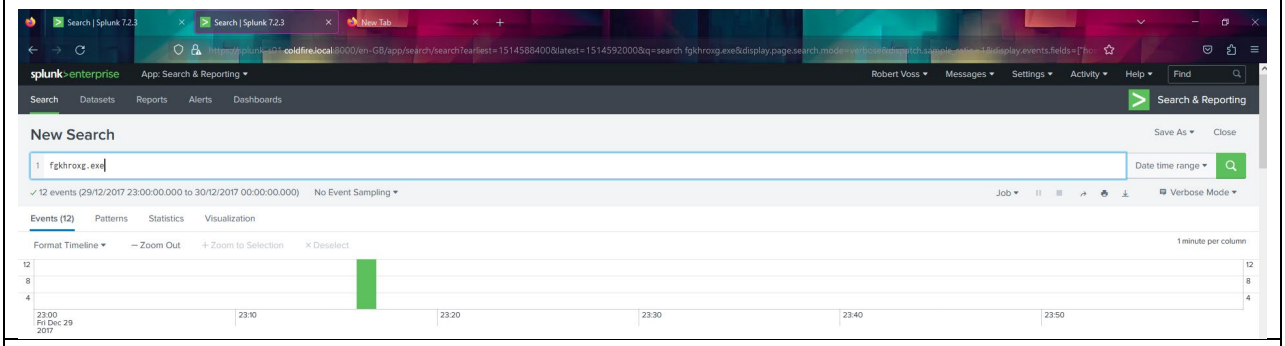


A new 8-character name appears…
fgkhroxg.exe

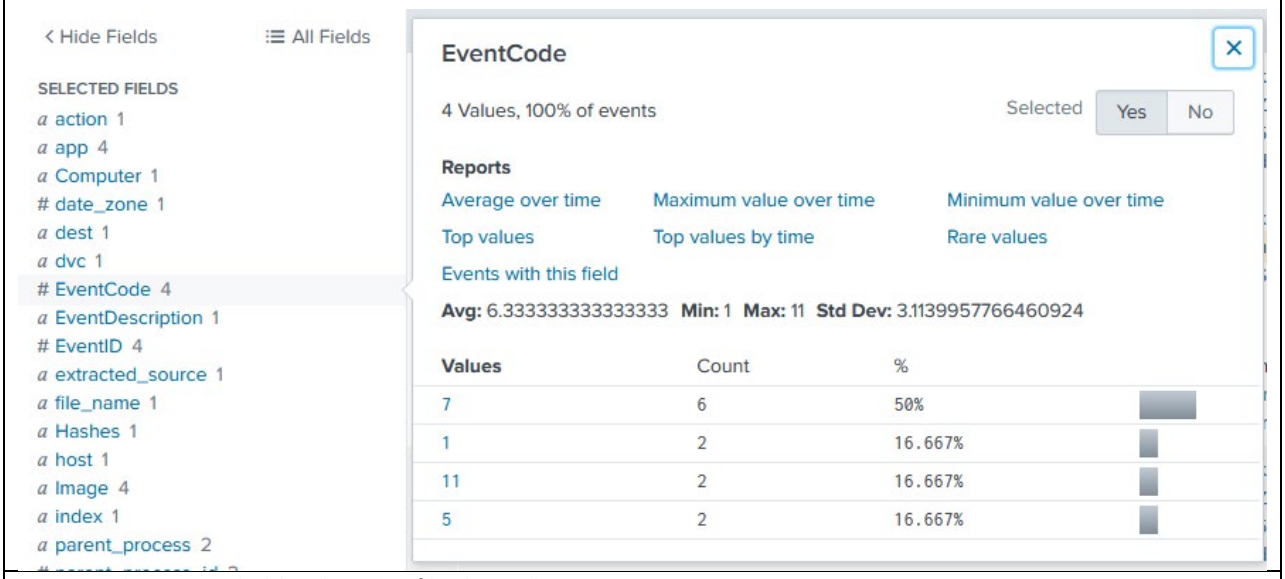
Now do the dance between Splunk and Atom

Copy fgkhroxg.exe and go into Splunk to see if there is any evidence of it

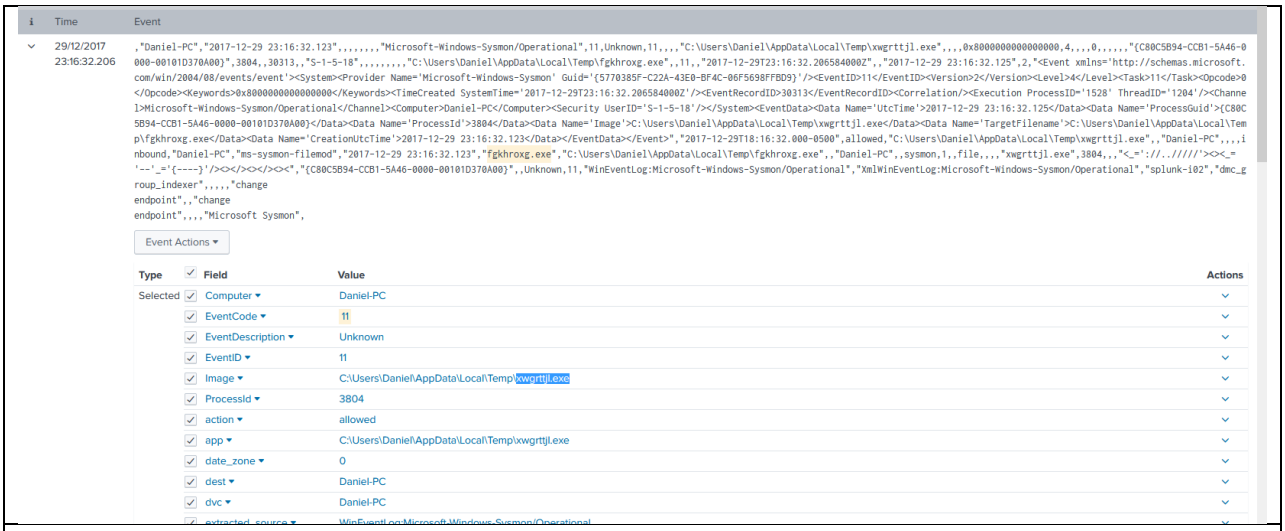
Save existing search (duplicate tab) before moving onto the new…



Check event codes with this file

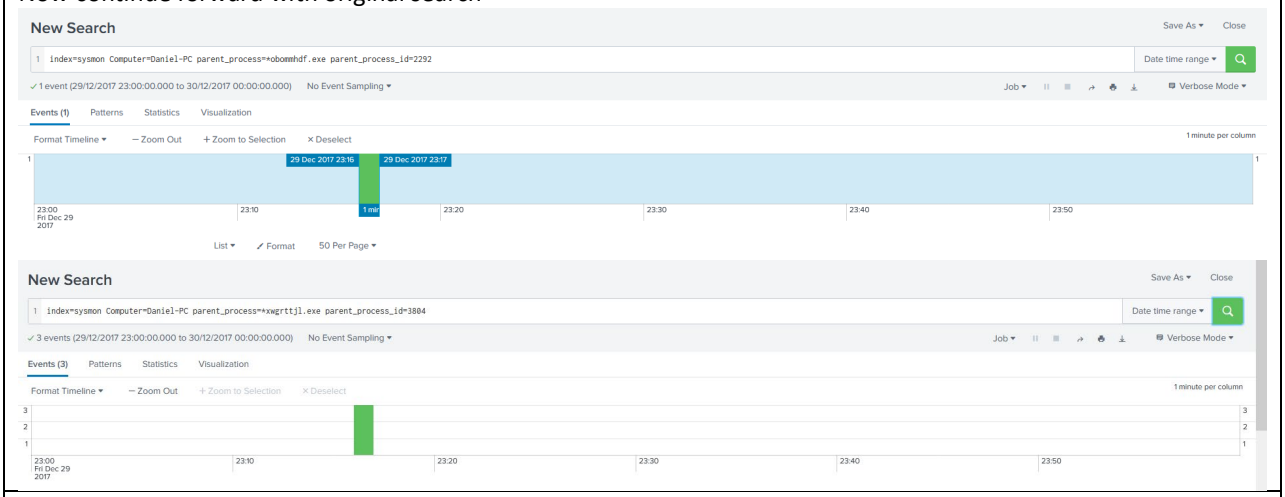


Event Code 11 – probably when this file showed up

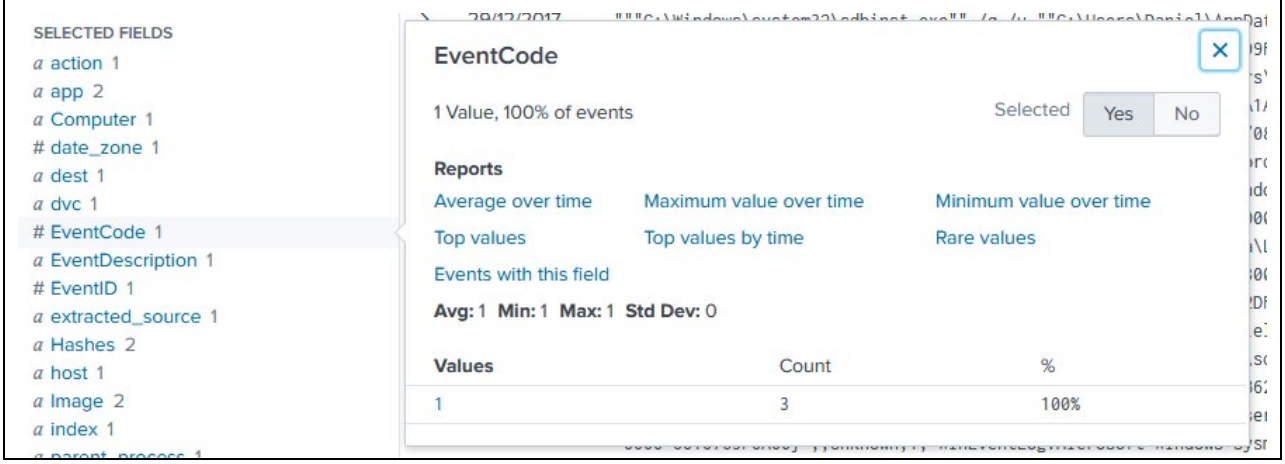


This shows that:
xwgrttjl.exe created fgkhroxg.exe

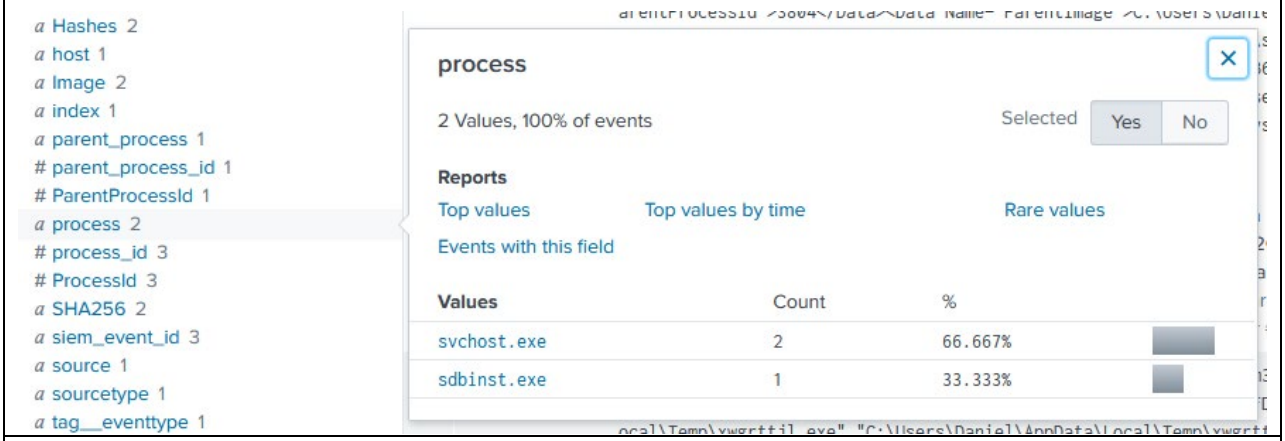
Now continue forward with original search



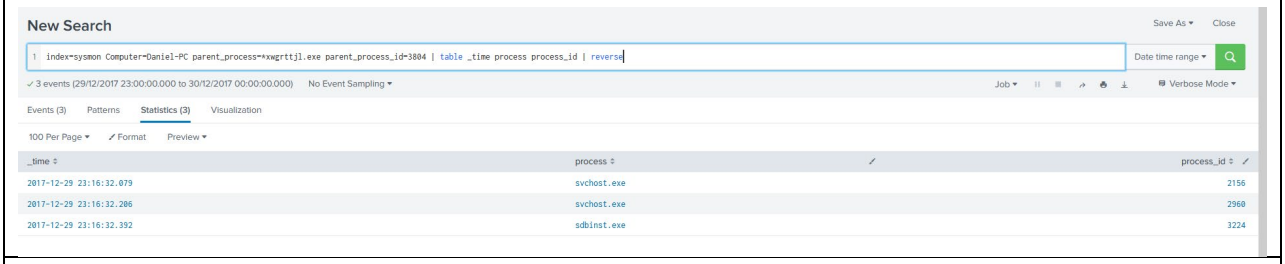
Shows that xwgrttjl.exe created 3 things



Check process



Set time search to list everything chronologically



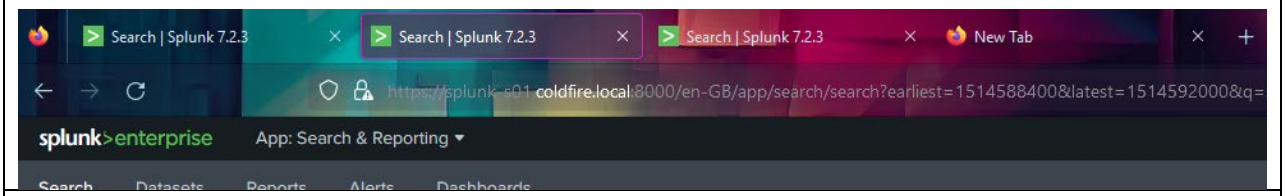
Repeat the above process with each newly identified processes…

svchost.exe (PID: 2156,
svchost.exe (PID: 2960,

sbdinst.exe (PID: 3224,

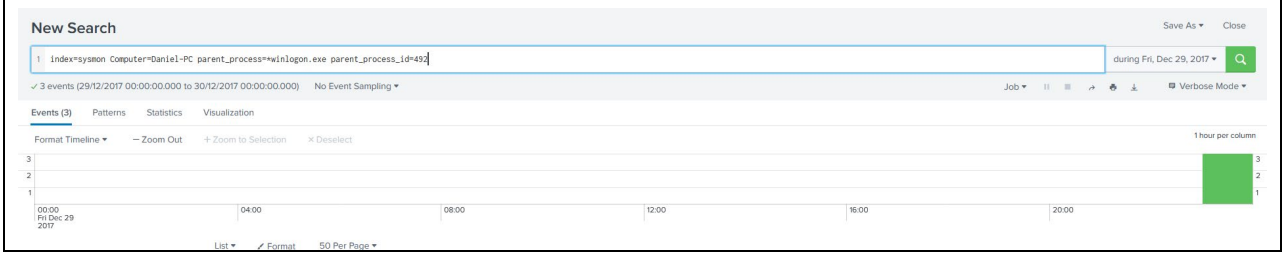
Now going back to verify that Winlogon didn't create anything elase

Duplicate tab to save current search which will be used to continue on moving forward…

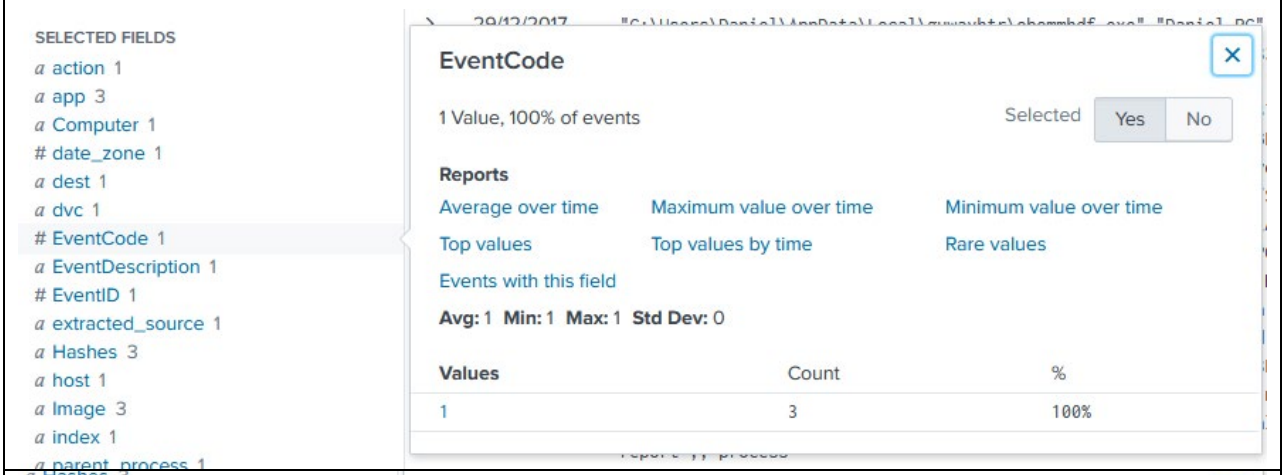


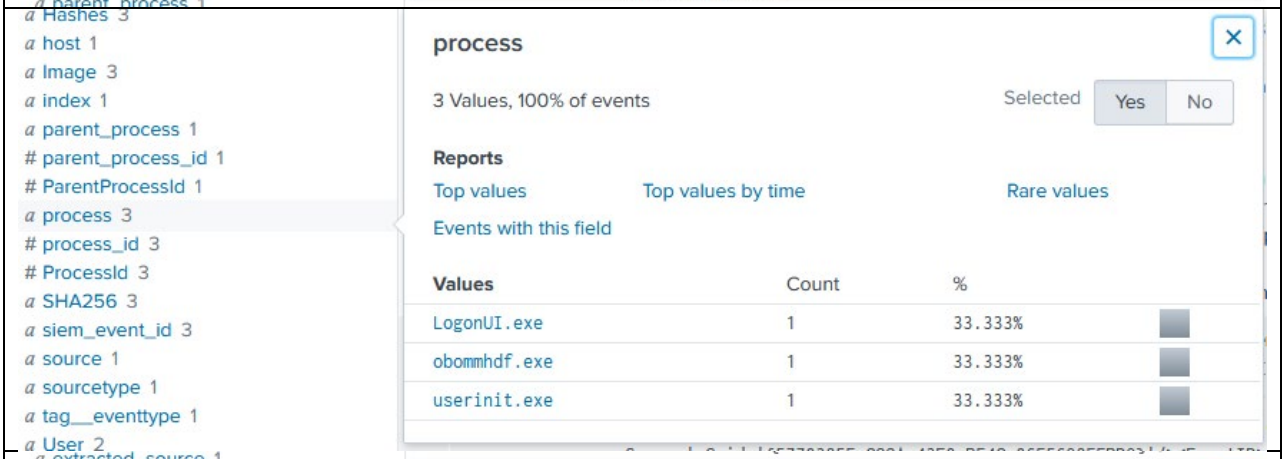
Rest time to full day to ensure proper coverage

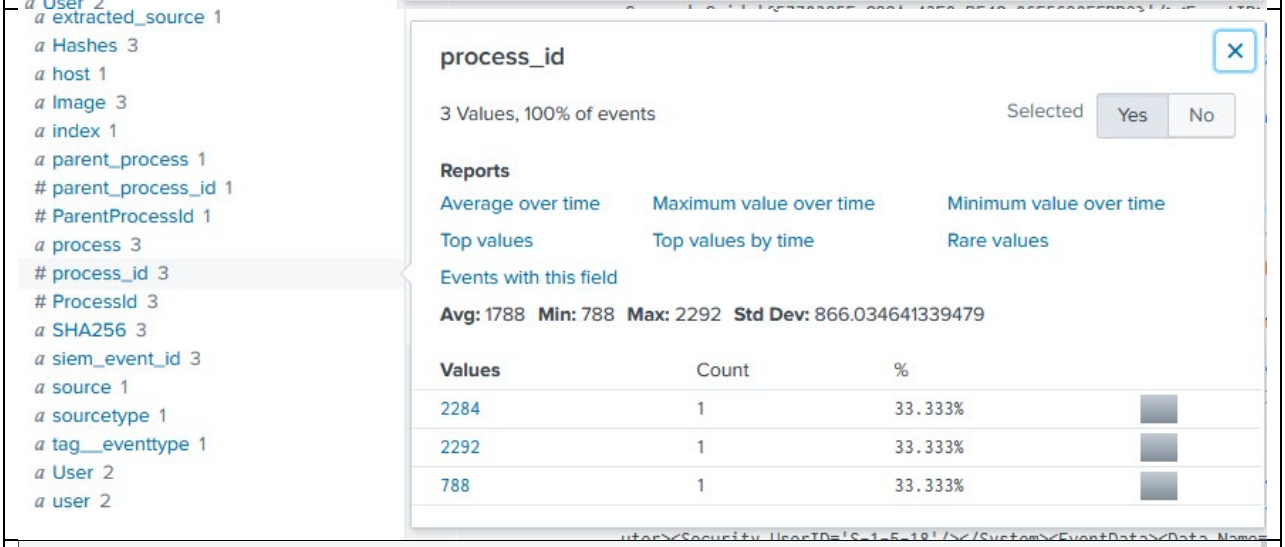
Change parent to winlogon

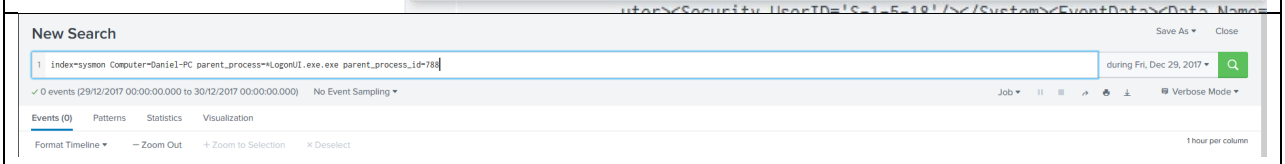


Winlogon created 3 process

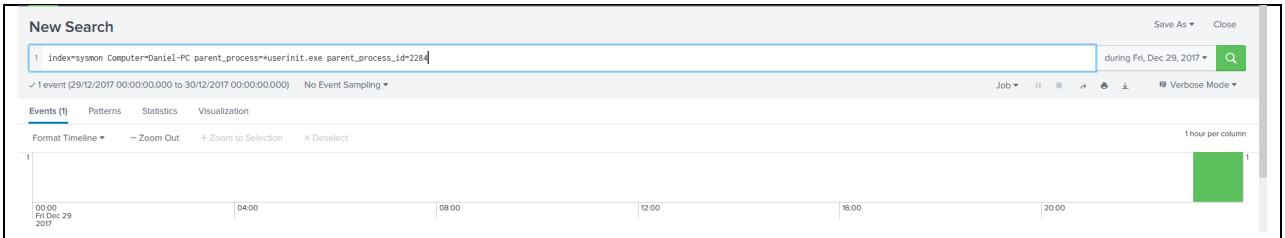




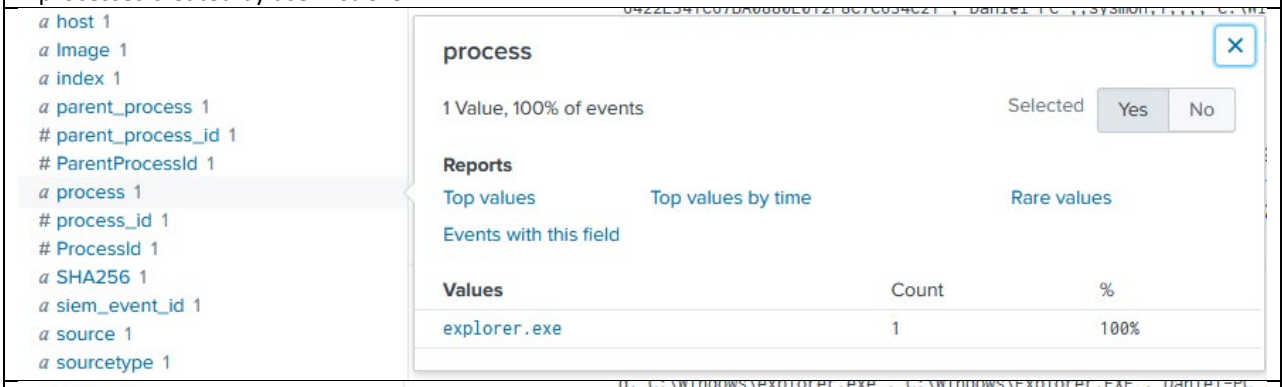


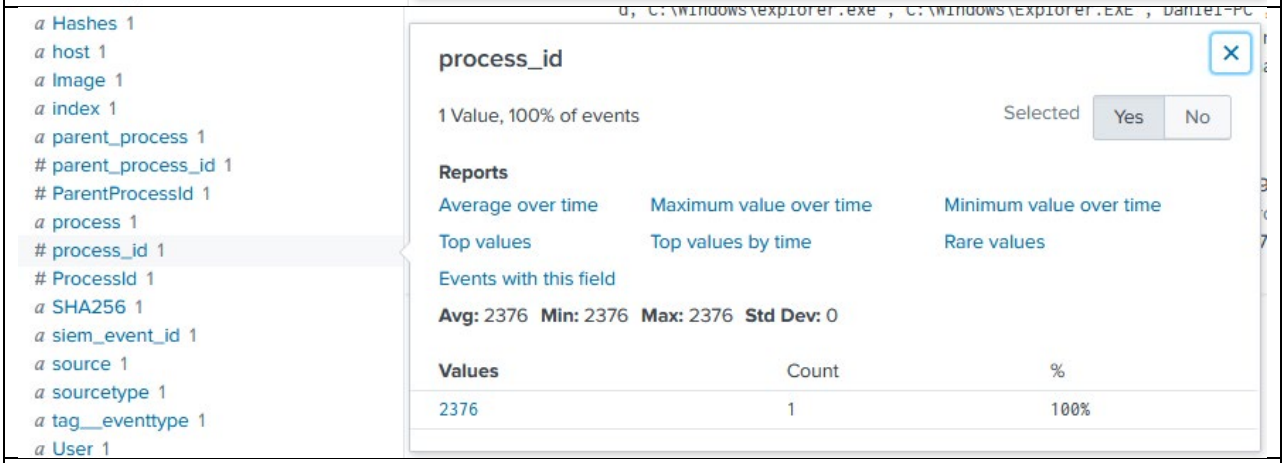


0 processes created by LogonUI.exe

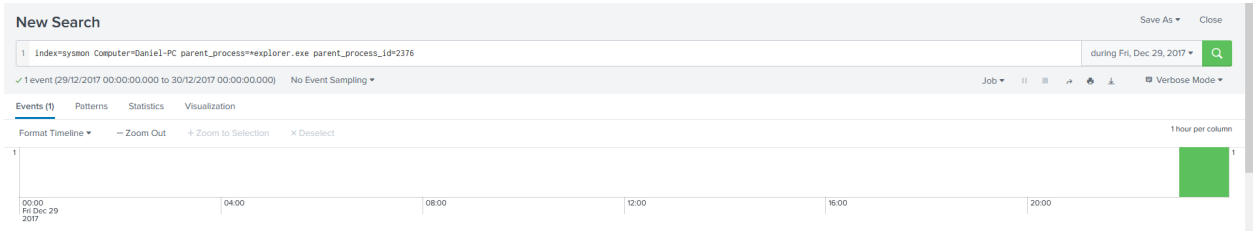


1 processes created by userinst.exe

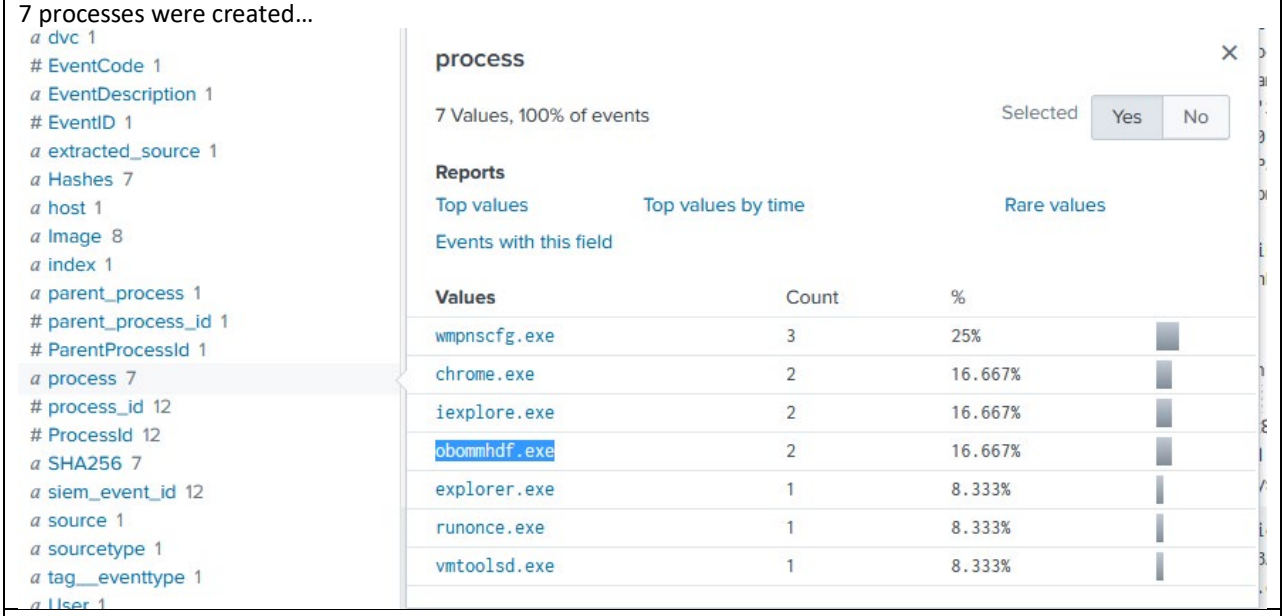




Continue search forward with Explorer and 2376



7 processes were created…



obommhdf.exe reappears…

investigate each process