



NIDS Hands-On

🔗 Done	✓
📅 Due Date	@09/21/2025
⚙️ Status	Done

- Utilize the SimSpace environment
- Utilize the index=ids
- Utilize the timeframe 6/25/2025 11:00:00 - 6/25/2025 11:50:00 (UTC Timezone)
- Utilize the knowledge you have from the proxy logs, alert, and IOCs.



How to Do a generic search on the ids index for the designated timeframe to analyze the alert signature IDs. How many events are there for signature ID 2031071?

ANSWER FORMAT: 123456 (Number Count)

HINT: You are going to need to use the stats command

`index=ids | stats count by alert.signature_id` OR

→ `index=ids alert.signature_id=2031071` → answer **4680**

New Search

index=ids alert.signature_id=2031071

✓ 4,680 events (6/25/25 11:00:00.000 AM to 6/25/25 11:50:00.000 AM) No Event Sampling ▼

Events (4,680) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

List ▼ Format 20 Per Page ▼

	i	Time	Event
< Hide Fields			
≡ All Fields			
SELECTED FIELDS			
a host 1			
a source 2			
a sourcetype 1			
INTERESTING FIELDS			
a alert.action 1			
a alert.category 1			
# alert.gid 1			
a alert.metadata.confidence{} 1			
a alert.metadata.created_at{} 1			
a alert.metadata.performance_impact{} 1			
a alert.metadata.signature_severity{} 1			
a alert.metadata.updated_at{} 1			
	>	6/25/25 11:49:59.827 AM	{ [-] alert: { [+] } app_proto: http community_id: 1:G8Tie2sp+Y8XbZiuiXbrlPcg4= dest_ip: 172.16.2.6 dest_port: 8080 direction: to_server event_type: alert flow_id: 2111799546564411 in_iface: bond0 packet: AAKzAAUBAAKzAAcCCABFAAAopNVAH8G+aysEAMnrBACBubYH5ArrQyCEom6E1AQIBQnI packet_info: { [+] } payload_printable: GET http://www.msftconnecttest.com/connecttest.txt HTTP/1 Cache-Control: no-cache

✂ How to Do a generic search on the ids index for the designated timeframe to analyze the alert signature IDs. How many events are there for signature alert ET INFO PE EXE or DLL Windows file download HTTP?

ANSWER FORMAT: 123456 (Number Count)

HINT: You are going to need to use the stats command

- To count by the descriptive signature name: `index=ids | stats count by alert.signature`
- To count by the numerical signature ID: `index=ids | stats count by alert.signature_id`
- For specific alert, use `index=ids "ET INFO PE EXE or DLL Windows file download HTTP"` → answer **2**

New Search

index=ids "ET INFO PE EXE or DLL Windows file download HTTP"

✓ 2 events (6/25/25 11:00:00.000 AM to 6/25/25 11:50:00.000 AM) No Event Sampling ▼

Events (2) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

List ▼ Format 20 Per Page ▼

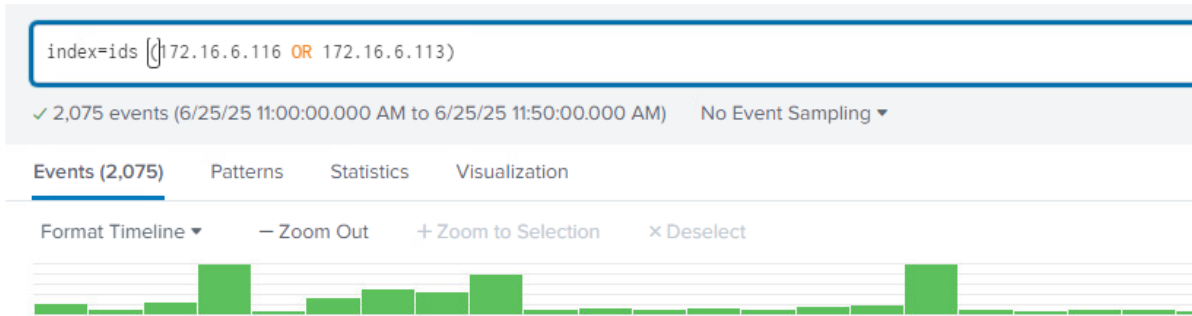
< Hide Fields	≡ All Fields	i	Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1 INTERESTING FIELDS a alert.action 1 a alert.category 1 # alert.gid 1 a alert.metadata.confidence{} 1 a alert.metadata.created_at{} 1 a alert.metadata.signature_severity{} 1 a alert.metadata.updated_at{} 1 # alert.rev 1 a alert.rule 1		>	6/25/25 11:19:31.744 AM	<pre>{ [-] alert: { [+] } app_proto: http community_id: 1:kxXEmhsTsqH0tjSLV+XTN26N1SQ= dest_ip: 172.16.6.116 dest_port: 60485 direction: to_client event_type: alert files: [[+]] flow_id: 848107553319256 in_iface: bond0 metadata: { [+] } packet: AAKzABgeAAKzAAcECABFAATArEJAAD8GK1usEAIC</pre>

✖ How to do a targeted string search for the IP addresses of the compromised systems on the ids index during the designated timeframe. How many events are there for both systems?

ANSWER FORMAT: 123456 (Number Count) HINT: You are going to need to use the stats command

- The target IPs are:
 - ACC Win 1016**, which corresponds to IP address 172.16.6.116 .
 - ACC Win 1013**, which corresponds to IP address 172.16.6.113

- `index=ids (172.16.6.116 OR 172.16.6.113)` → answer = **2009**



✂ How to Do a targeted string search for the (2) known bad IP addresses identified in the ids index during the designated timeframe. How many events are there for both IP addresses?

ANSWER FORMAT: 123456 (Number Count)

HINT: You are going to need to use the stats command. You won't find one of the domains just by searching

`index=ids (23.192.51.165 OR 162.241.253.54)` - answer = **12**

dest_IP

39 Values, 100% of events

Yes No

Reports

Top values Top values by
time Rare values

Events with this field

Top 10 Values

Count

172.16.2.8

Src_IP

Top 10 Values	Count	%
172.16.6.122	1,144	3.12%
172.16.6.107	1,121	3.058%
172.16.6.106	1,106	3.017%
172.16.6.103	1,095	2.987%
172.16.6.124	1,093	2.981
172.16.6.101	1,088	2.968%

30,833 84.101%
 172.16.2.6 5,
 331 14. 541%
 23.192.51.165 408
 1.113%
 162.241.253.54 11
 0.03%
 162.241 .252.54 5
 0.014%
 172.16.6.114 5
 0.014%
 172.16.6.105 3
 0.008%
 172.16.6.109 3
 0.008%
 172.16.6.111 3
 0.008%
 172.16.6.116 3
 0.008%]

172.16.6.111	1,087	2.965%
172.16.6.119	1,086	2.962%
172.16.6.126	1,084	2.957%
172.16.6.102	1,079	2.943%

New Search

index=ids (23.192.51.165 OR 162.241.253.54)

✓ 419 events (6/25/25 11:00:00.000 AM to 6/25/25 11:50:00.000 AM) No Event Sampling ▼

Events (419) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

4 Fields Fields

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS

List ▼ Format 20 Per Page ▼

i	Time	Event
>	6/25/25 11:37:07.791 AM	<pre>{ [-] alert: { [+] } app_proto: http community_id: 1:gJNx7DaxBbN+TqQI3PXWxnYWprI= dest_ip: 162.241.253.54</pre>

- ❌ How to Do a targeted string search for the known malicious binary file (exe) in the ids index during the designated timeframe. Review the payload. What was the length of the content downloaded?

ANSWER FORMAT: 123456 (Amount)

- I ran `index=ids "ET INFO PE EXE or DLL Windows file download HTTP"` → I looked under `files.filename` and **/QRCodeScanner.exe** which is a Indicator of Compromise (IOC)

The screenshot shows a search interface with a list of fields on the left and a search results panel on the right. The field `files.filename` is selected. The search results panel shows a table with the following data:

Values	Count	%
/QRCodeScanner.exe	2	100%

- now I do `index=ids "QRCodeScanner.exe"`
- `payload_printable` field, which contains readable data from the network packet → `Content-Length` → answer = **5608448**

The screenshot shows a search interface with a list of fields on the left and a search results panel on the right. The field `payload_printable` is selected. The search results panel shows a table with the following data:

Values
HTTP/1.1 200 OK Server: nginx/1.24.0 Date: Wed, 25 Jun 2025 11:19:33 GMT Content-Type: application/octet-stream Content-Length: 5608448 Connection: keep-alive Last-Modified: Wed, 25 Jun 2025 11:19:29 GMT

✖ How to do a targeted string search for the known compromised system and/or the known malicious domains or IP addresses in the ids index during the designated timeframe. Review the payload. It appears system reconnaissance has been performed. What is the Volume Serial Number identified for the C:\ in ACC-WIN10-16?

ANSWER FORMAT: 1234-A1B2 (Use CAPS for letters)

I will use → `index=ids 172.16.6.116 "Volume Serial Number"` → `payload_printable` → **answer= 0258-91D4**

```
POST /update HTTP/1.1 User-Agent: Mozilla/5.0 1
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/74.0.3729.169
Safari/537.36 Content-Length: 955 Content-Type:
text/plain Accept-Encoding: gzip Host: saltybug.com
Via: 1.1 ["site-proxy.site.lan"] (squid/3.5.27) X-
Forwarded-For: 172.16.6.116 Cache-Control: max-
age=259200 Connection: keep-alive ip=172.16.6.116
10.10.6.116 hid=2 hn=acc-win10-16 tid=4 Volume in
drive C has no label. Volume Serial Number is 0258-
91D4 Directory of C:\ 06/24/2025 06:56 PM 2,997
edge_exported.xml 06/18/2025 08:44 AM <DIR> Microsoft
12/07/2019 05:14 AM <DIR> PerfLogs 06/13/2025 10:57
AM <DIR> Program Files 04/22/2025 03:44 PM <DIR>
Program Files (x86) 11/21/2022 10:12 PM 31,908,355
SystemInit-Fix_2016_Autologon.exe 11/30/2022 07:50 PM
40,481,427 SystemInit-puppet7.exe 06/18/2025 12:00 PM
<DIR> temp 04/17/2025 03:18 PM <DIR> tmp 06/13/2025
08:04 AM <DIR> Users 11/21/2022 10:34 PM 5,211,080
vcredist_x64.exe 11/22/2022 12:19 PM 4,483,040
vcredist_x86.exe 06/13/2025 04:51 PM <DIR> Windows 5
File(s) 82,086,899 bytes 8 Dir(s) 46,795,595,776
bytes free
```



How to do a targeted string search for the known compromised system and/or the known malicious domains or IP addresses in the ids index during the designated timeframe. Review the payload. It appears system reconnaissance has been performed. What was the process ID (PID) for svchost.exe in ACC-WIN10-16?

ANSWER FORMAT: 123 (Process ID)

index=ids 172.16.6.116 "svchost.exe" → payload_printable → task_list

```
POST http://saltybug.com/update HTTP/1.1 Host:
saltybug.com User-Agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/74.0.3729.169 Safari/537.36 Connection:
close Content-Length: 37252 Content-Type: text/plain
Accept-Encoding: gzip ip=172.16.6.116 10.10.6.116
hid=2 hn=acc-win10-16 tid=11 Image Name PID Session
Name Session# Mem Usage Status User Name CPU Time
Window Title =====
=====
=====
=====
=====
=====
===== System Idle Process 0 Services 0
8 K Unknown NT AUTHORITY\SYSTEM 0:29:43 N/A System 4
Services 0 144 K Unknown N/A 0:00:51 N/A Registry 92
Services 0 29,456 K Unknown NT AUTHORITY\SYSTEM
0:00:04 N/A smss.exe 352 Services 0 988 K Unknown NT
AUTHORITY\SYSTEM 0:00:00 N/A csrss.exe 456 Services 0
5,276 K Unknown NT AUTHORITY\SYSTEM 0:00:01 N/A
wininit.exe 560 Services 0 6,712 K Unknown NT
AUTHORITY\SYSTEM 0:00:00 N/A csrss.exe 568 Console 1
5,324 K Running NT AUTHORITY\SYSTEM 0:00:00 N/A
winlogon.exe 660 Console 1 11,428 K Unknown NT
AUTHORITY\SYSTEM 0:00:00 N/A services.exe 676
Services 0 13,644 K Unknown NT AUTHORITY\SYSTEM
0:00:05 N/A lsass.exe 716 Services 0 20,556 K Unknown
NT AUTHORITY\SYSTEM 0:00:14 N/A svchost.exe 808
Services 0 27,656 K Unknown NT AUTHORITY\SYSTEM
0:00:02 N/A fontdrvhost.exe 832 Services 0 2,552 K
Unknown Font Driver Host\UMFD-0 0:00:00 N/A
fontdrvhost.exe 872 Console 1 9,812 K Unknown Font
Driver Host\UMFD-1 0:00:01 N/A svchost.exe 936
Services 0 16,588 K Unknown NT AUTHORITY\NETWORK
SERVICE 0:00:03 N/A svchost.exe 988 Services
```

answer=936 I will go with the first instance


```
ip=172.16.6.116 10.10.6.116
hid=2
hn=acc-win10-16
tid=11
```

Image Name	PID	Session Name	Session#	Mem Usage	Status	User Name	CPU Time	Window Title
System Idle Process	0	Services	0	8 K	Unknown	NT AUTHORITY\SYSTEM	0:29:43	N/A
System	4	Services	0	144 K	Unknown	N/A	0:00:51	N/A
Registry	92	Services	0	29,456 K	Unknown	NT AUTHORITY\SYSTEM	0:00:04	N/A
smss.exe	352	Services	0	988 K	Unknown	NT AUTHORITY\SYSTEM	0:00:00	N/A
csrss.exe	456	Services	0	5,276 K	Unknown	NT AUTHORITY\SYSTEM	0:00:01	N/A
wininit.exe	560	Services	0	6,712 K	Unknown	NT AUTHORITY\SYSTEM	0:00:00	N/A
csrss.exe	568	Console	1	5,324 K	Running	NT AUTHORITY\SYSTEM	0:00:00	N/A
winlogon.exe	660	Console	1	11,428 K	Unknown	NT AUTHORITY\SYSTEM	0:00:00	N/A
services.exe	676	Services	0	13,644 K	Unknown	NT AUTHORITY\SYSTEM	0:00:05	N/A
lsass.exe	716	Services	0	20,556 K	Unknown	NT AUTHORITY\SYSTEM	0:00:14	N/A
svchost.exe	808	Services	0	27,656 K	Unknown	NT AUTHORITY\SYSTEM	0:00:02	N/A
fontdrvhost.exe	832	Services	0	2,552 K	Unknown	Font Driver Host\UMFD-0	0:00:00	N/A
fontdrvhost.exe	872	Console	1	9,812 K	Unknown	Font Driver Host\UMFD-1	0:00:01	N/A
svchost.exe	936	Services	0	16,588 K	Unknown	NT AUTHORITY\NETWORK SERVICE	0:00:03	N/A



How to do a targeted string search for the known compromised system and/or the known malicious domains or IP addresses in the ids index during the designated timeframe. Review the payload. It appears system reconnaissance has been performed. What time did the outbound netstat alert trigger for ACC-WIN10-16?

ANSWER FORMAT: YYYY-MM-DD hh:mm:ss (remember UTC)

```
index=ids 172.16.6.116 "netstat"
```

→ **answer=2025-06-25 11:30:44**

its this answer because its the earliest alert

```
2025-06-25T11:30:44.408779+0000
```

```
2025-06-25T11:30:44.409794+0000
```

```
2025-06-25T11:37:07.791853+0000
```

```
2025-06-25T11:37:07.792938+0000
```



How to do a targeted string search for the known compromised system and/or the known malicious domains or IP addresses in the ids index during the designated timeframe. Review the payload. It appears system reconnaissance has been performed. User accounts appear to be exfiltrated from \\site-dc.site.lan. Which user is the last account listed?

ANSWER FORMAT: user.name

▼ I did `index=ids 172.16.6.116 "accounts"` and got 4 events. the last name was **zackary.warren**

```
6/25/25
11:34:48.132 AM
{ [-]
  alert: { [+]
  }
  app_proto: http
  community_id: 1:hIOKhZQflhBG7Bg+qSYjkbtcOV4=
  dest_ip: 172.16.2.6
  dest_port: 8080
  direction: to_server
  event_type: alert
  files: [ [+]
  ]
  flow_id: 2204090579695139
  in_iface: bond0
  packet: AAKzAAcEAAKzABgeCABFAAAoFhBAAIAGhCWsEAZ0rBACBu4
HH5CqBcn3TQPJ0IARBAGyzAAAAAAAAAAAA
  packet_info: { [+]
  }
  payload_printable: POST http://saltybug.com/update HTTP/1.1
Host: saltybug.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.
36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36
Connection: close
Content-Length: 2685
Content-Type: text/plain
Accept-Encoding: gzip

ip=172.16.6.116 10.10.6.116
hid=2
hn=acc-win10-16
```

tid=21

The request will be processed at a domain controller for domain site.lan.

User accounts for \\site-dc.site.lan

\$E71000-GQRP1NRQ2VPA Administrator ahmed.ortega
alina.beck alvin.shelton b-admin0
billie.acosta bob.burke brock.morgan
carla.rush celia.moody chandler.steele
chandra.perez charity.bowen charles.hardy
charley.fritz chelsea.gillespie cheri.freeman
christopher.mejia christy.foster ciara.schultz
cierra.ray dale.hays darryl.richmond
dewey.houston dominic.monroe doris.ford
elias.small eric.blair erwin.mullins
eunice.gilmore freddie.mclaughlin gavin.horn
george.webster Guest i-admin0
irwin.choi janice.durham jaron.olsen
jefferson.livingston jessica.zuniga joanna.wilkerson
joaquin.clayton josh.brock karen.adkins
katharine.stone kenneth.hodge krbtgt
lara.whitaker laurel.harding liam.sherman
loren.holder louise.andersen lucy.alexander
madelyn.luna makenzie.melton marcos.casey
maya.goodman michelle.blanchard monroe.thompson
nelda.rios norma.finley o-admin0
ola.burch omar.gilbert phil.joyce
r-admin0 randolph.hickman ricardo.barr
robyn.juarez rosemary.cortez roxanne.farley
sadie.villa sean.wilkinson sebastian.wells
sheryl.trevino silas.stuart SM_0b5ccbeb90f548a19
SM_6ed8e1912ef649de9 SM_9875ff9f2a2c414eb SM_9d0d92fc4077
45b2b

```
SM_9d5429faa38348d3b SM_df76960b01504ed59 SM_f00c10eb0b0
34bea8
SM_fa9d6043c3b74cd1a SM_fd632d5705984a639 sshd
summer.hayes tanner.grant tessa.church
thomas.michael triston.beltran zackary.warren
The command completed successfully.
```

✖ How to do a targeted string search for the known compromised system and/or the known malicious domains or IP addresses in the ids index during the designated timeframe. Review the payload. It appears system reconnaissance has been performed. When was the first time the alert 'ET MALWARE Windows dir Microsoft Windows DOS prompt command exit OUTBOUND' was triggered on ACC-WIN10-16?

ANSWER FORMAT: YYYY-MM-DD hh:mm:ss

The following Splunk command will find the relevant events, filter them for the specific alert signature, and then sort them to find the earliest occurrence:

```
index=ids "ACC-WIN10-16" "ET MALWARE Windows dir Microsoft Windows DOS prompt command exit OUTBOUND" |
sort _time → answer= 2025-06-25 11:22:08
```

i	Time	Event
>	6/25/25 11:22:08.003 AM	{ [-] alert: { [+] } app_proto: http community_id: 1:8ass47OW7Ue3OG4VF3bI/PnkdT0= dest_ip: 162.241.253.54 dest_port: 80 direction: to_server event_type: alert files: [[+]] flow_id: 2229932599955735 in_iface: bond0 packet: AAKzAAcCAAKzAAUBCABFAAA0PEdAAEAGsD6sEAIGovH9Nrt+AFBGerJdF2nLLIAQAFUocQAAAQEICnEMQHz2vVFH packet_info: { [+]

✖ How to do a targeted string search for the alert signature 'ET INFO Windows PowerShell User-Agent Usage' in the ids index during the designated timeframe. Review the payload. What was the signature ID for the alert?

ANSWER FORMAT: 1234567 (signature)

`index=ids "ET INFO Windows PowerShell User-Agent Usage"` → **answer=2033355**



✖ How to do a targeted string search for the alert signature 'ET INFO Windows PowerShell User-Agent Usage' in the ids index during the designated timeframe. Review the payload. When was the first time the alert was triggered?

ANSWER FORMAT: YYYY-MM-DD hh:mm:ss

I do this command and record 1st alert triggered

`index=ids "ET INFO Windows PowerShell User-Agent Usage" | sort _time` → **answer= 2025-06-25 11:44:15**

index=ids "ET INFO Windows PowerShell User-Agent Usage" | sort _time

✓ 4 events (6/25/25 11:00:00.000 AM to 6/25/25 11:50:00.000 AM) No Event Sampling ▼

Events (4) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

List ▼ Format 20 Per Page ▼

< Hide Fields	≡ All Fields	i	Time	Event
SELECTED FIELDS		>	6/25/25 11:44:15.764 AM	{ [-] alert: { [+] } app_proto: http community_id: 1:ppLKkxu3wvfIPE1D/f2tz217rAQ=
a host 1				
a source 1				
a sourcetype 1				

✖ How to do a targeted string search for the alert signature 'ET INFO Windows PowerShell User-Agent Usage' in the ids index during the designated timeframe. Review the payload. What internal client host is involved in the alert?

ANSWER FORMAT: host-name-01 (all lowercase) → **answer=acc-win10-13**

✖ How to do a targeted string search for the alert signature 'ET INFO Windows PowerShell User-Agent Usage' in the ids index during the designated timeframe. Review the payload. How many ACTUAL events are coming from the client system?

ANSWER FORMAT: 1 (a number)

index=ids "ET INFO Windows PowerShell User-Agent Usage" "172.16.6.113" →, the four events logged are not four separate, independent actions. Instead, they represent two distinct network sessions, each generating two log entries. This happens because the network security monitoring tools are logging the traffic at two different points: so **answer=2**



How to do a targeted string search for the alert signature 'ET INFO Windows PowerShell User-Agent Usage' in the ids index during the designated timeframe. Review the payload. What is the external IP address involved in the alert?

ANSWER FORMAT: 1.2.3.4

`index=ids "ET INFO Windows PowerShell User-Agent Usage"` → **answer= 162.241.252.54**

```
> 6/25/25      { [-]
    11:44:15.764 AM    alert: { [+]
                        }
                        app_proto: http
                        community_id: 1:ppLKkxu3wvfIPE1D/f2tz217rAQ=
                        dest_ip: 162.241.252.54
                        dest_port: 80
                        direction: to_server
```



How to do a targeted string search for the alert signature 'ET INFO Windows PowerShell User-Agent Usage' in the ids index during the designated timeframe. Review the payload. There appears to be a new interesting domain based on this activity. What is the domain?

ANSWER FORMAT: domain.com

`index=ids "ET INFO Windows PowerShell User-Agent Usage"` → **answer= s4ltybug.com**