New Search

```
sourcetype=_json datasource=sysmon event.code=22
| search dns.question.name="*.finance" OR dns.question.name="*.xyz"
```

Last 24 hours

✓ **4 events** (12/13/25 5:00:00.000 AM to 12/14/25 5:28:21.000 AM) No Event Sampling

Events (4)

Format Timeline

1 hour per column

SELECTED FIELDS

- *a* host 1
- *a* source 1
- *a* sourcetype 1

INTERESTING FIELDS

- *a* datasource 1
- *a* dns.answers.data 2
- *a* dns.question.name 1
- *a* dns.resolved_ip 1
- *a* event.action 1
- # event.code 1
- *a* host.name 4
- *a* index 1
- # linecount 1
- *a* network.protocol 1
- *a* process.name 1
- # process.pid 4
- *a* punct 1
- *a* splunk_server 1
- *a* timestamp 4

+ Extract New Fields (/en-US/app/search/field_extractor?sid=1765690101.260)

Time	Event
12/14/25 4:40:12.369 AM	see below

Time: 12/14/25 4:40:12.369 AM

```
{ [-]
   datasource: sysmon
   dns.answers.data: mail.tryhatme.finance, 34.24g
4.197.202
   dns.question.name: autodiscover.tryhatme.finance
   dns.resolved_ip: 34.244.197.202
   event.action: Dns query (rule: DnsQuery)
   event.code: 22
   host.name: win-3454
   network.protocol: dns
   process.name: OUTLOOK.EXE
   process.pid: 3648
   timestamp: 12/14/2025 04:40:12.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time: 12/14/25 4:37:55.369 AM

```
{ [-]
   datasource: sysmon
   dns.answers.data: mail.tryhatme.finance, 34.244.
197.202
   dns.question.name: autodiscover.tryhatme.finance
   dns.resolved_ip: 34.244.197.202
   event.action: Dns query (rule: DnsQuery)
   event.code: 22
   host.name: win-3449
   network.protocol: dns
   process.name: OUTLOOK.EXE
   process.pid: 3587
   timestamp: 12/14/2025 04:37:55.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time Event

12/14/25
4:29:36.369 AM

```
{ [-]
   datasource: sysmon
   dns.answers.data: mail.tryhatme.finance, 34.24g
4.197.202
   dns.question.name: autodiscover.tryhatme.finance
   dns.resolved_ip: 34.244.197.202
   event.action: Dns query (rule: DnsQuery)
   event.code: 22
   host.name: win-3458
   network.protocol: dns
   process.name: OUTLOOK.EXE
   process.pid: 3906
   timestamp: 12/14/2025 04:29:36.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

12/14/25
4:27:47.369 AM

```
{ [-]
   datasource: sysmon
   dns.answers.data: mail.tryhatme.finance, 34.24g
4.197.202
   dns.question.name: autodiscover.tryhatme.finance
   dns.resolved_ip: 34.244.197.202
   event.action: Dns query (rule: DnsQuery)
   event.code: 22
   host.name: win-3455
   network.protocol: dns
   process.name: OUTLOOK.EXE
   process.pid: 3600
   timestamp: 12/14/2025 04:27:47.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json