# New Search

```
sourcetype=_json datasource=email direction=inbound
| search content="*Bitcoin*" OR content="*inheritance*" OR content="*banking*"
```

Last 24 hours

✓ **3 events** (12/13/25 5:00:00.000 AM to 12/14/25 5:29:03.000 AM) No Event Sampling

**Events (3)**

Format Timeline

1 hour per column

**SELECTED FIELDS**

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

**INTERESTING FIELDS**

| | | |
|---|---|---|
| *a* | attachment | 1 |
| *a* | content | 2 |
| *a* | datasource | 1 |
| *a* | direction | 1 |
| *a* | index | 1 |
| # | linecount | 1 |
| *a* | punct | 2 |
| *a* | recipient | 3 |
| *a* | sender | 3 |
| *a* | splunk_server | 1 |
| *a* | subject | 2 |
| *a* | timestamp | 3 |

+ Extract New Fields (/en-US/app/search/field_extractor?sid=1765690143.261)

| Time | Event |
|---|---|
| 12/14/25<br>4:43:02.369 AM | { [-]<br>**attachment**: None<br>**content**:  Our exclusive system guarantees instant Bitcoin doubling Send us just 100 and watch it turn into 200 instantly<br>**datasource**: email<br>**direction**: inbound<br>**recipient**: diego.summers@tryhatme.com<br>**sender**: tim@headweartrendsetters.org<br>**subject**: Instant Wealth Send Bitcoin to Double Your Money<br>**timestamp**: 12/14/2025 04:43:02.369<br>}<br>Show as raw text<br>host = 10.10.106.238:8989 source = eventcollector sourcetype = _json |
| 12/14/25<br>4:24:06.369 AM | { [-]<br>**attachment**: None<br>**content**:  A long lost billionaire relative has left you their secret hat empire To claim your inheritance send us your banking details immediately<br>**datasource**: email<br>**direction**: inbound<br>**recipient**: support@tryhatme.com<br>**sender**: eileen@trendymillineryco.me<br>**subject**: Inheritance Alert: Unknown Billionaire Relative Left You Their Hat Fortunes<br>**timestamp**: 12/14/2025 04:24:06.369<br>}<br>Show as raw text<br>host = 10.10.106.238:8989 source = eventcollector sourcetype = _json |

| Time | Event |
|---|---|
| 12/14/25<br>4:23:35.369 AM | See the event below |

```
{ [-]
   attachment: None
   content:  Our exclusive system guarantees instant Bitcoin doubling Send us just 100 and watch it turn into 200 instantly
   datasource: email
   direction: inbound
   recipient: armaan.terry@tryhatme.com
   sender: howe@headwearmarketwatch.org
   subject: Instant Wealth Send Bitcoin to Double Your Money
   timestamp: 12/14/2025 04:23:35.369
}
```

Show as raw text

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