Two hip-hop artists, Dwake and Present, are in the midst of a musical feud. Following long-stewing tensions between the artists, they have begun taking jabs at each other through their music.

Dwake, who is signed with OWL Records, was the first to strike. His newest song was intended to insult his arch-nemesis, Present, who is signed with Dollar Currency Records. However, he made a crucial mistake in his verse that took the feud in a different direction.

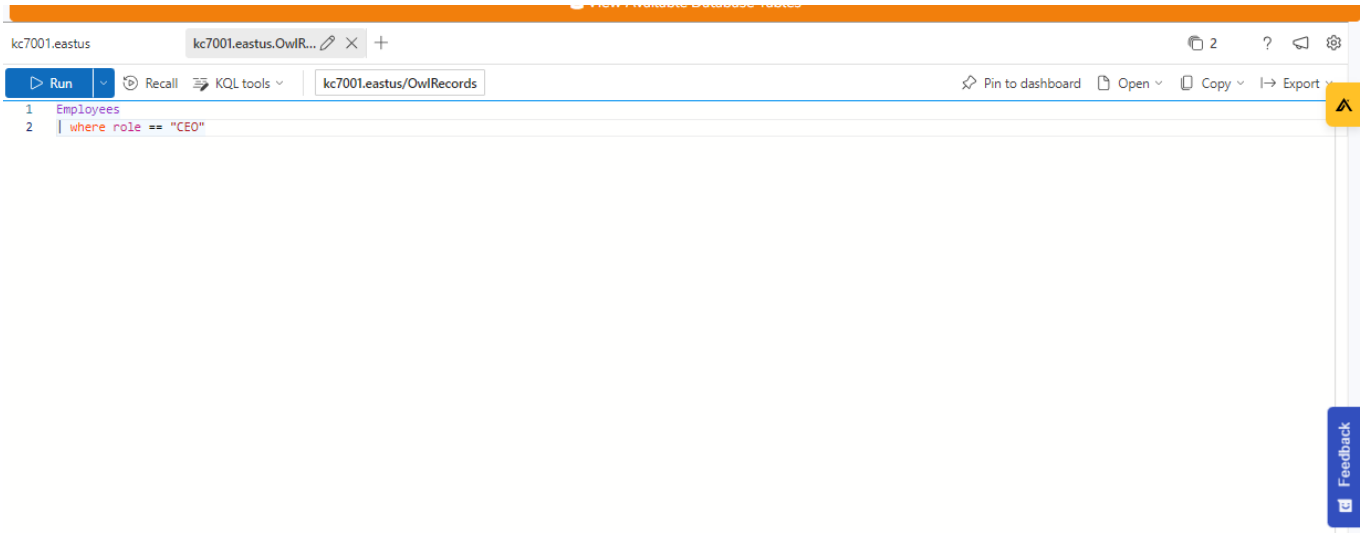
As a Security Analyst for OWL Records, your job is to keep the company's information safe so your artists don't get exposed during this ongoing feud.

Type `ready` to get started

ready

Solved by 3766 players || Need help? Ask on discord @ kc7cyber/community

Submit


kc7001.eastus
kc7001.eastus.OwlR...
Run
Recall
KQL tools
kc7001.eastus/OwlRecords
Pin to dashboard
Open
Copy
Export
1 Employees
2 | where role == "CEO"
Feedback

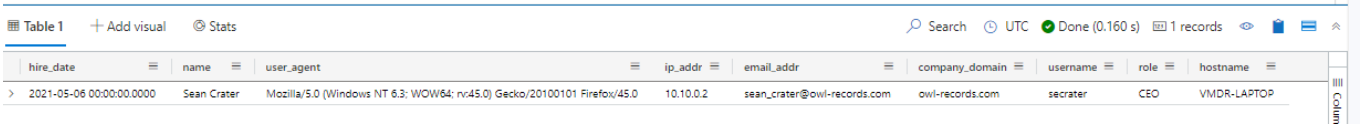
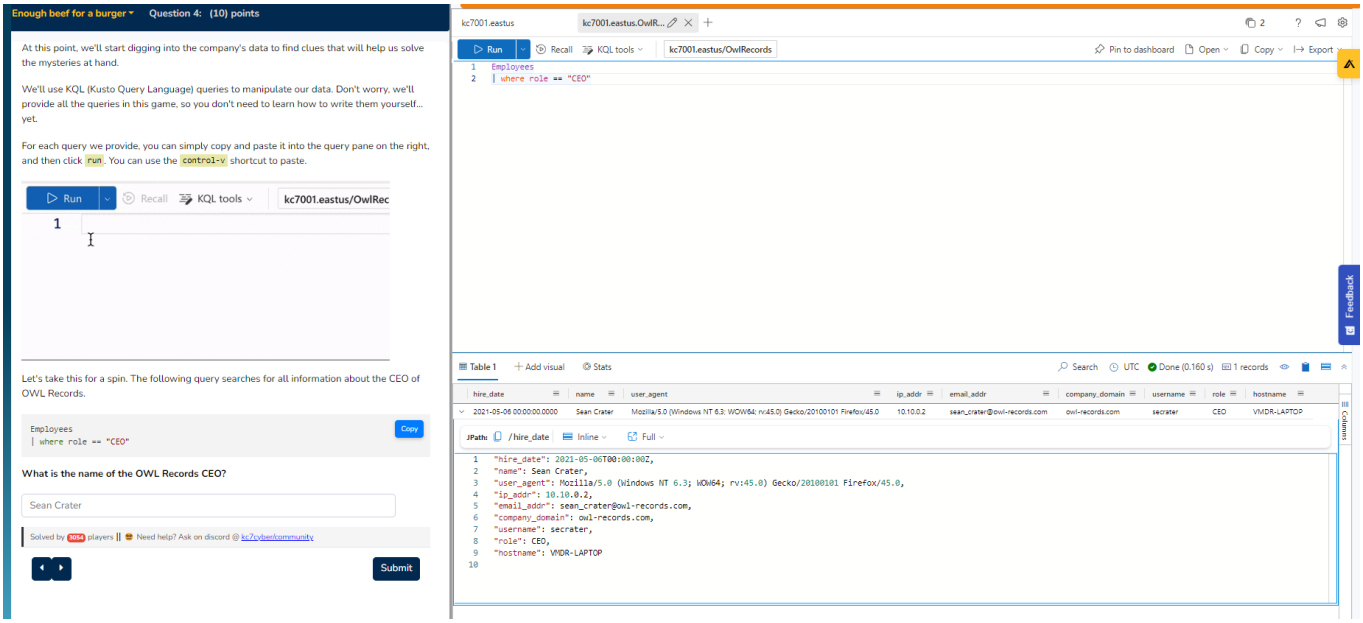
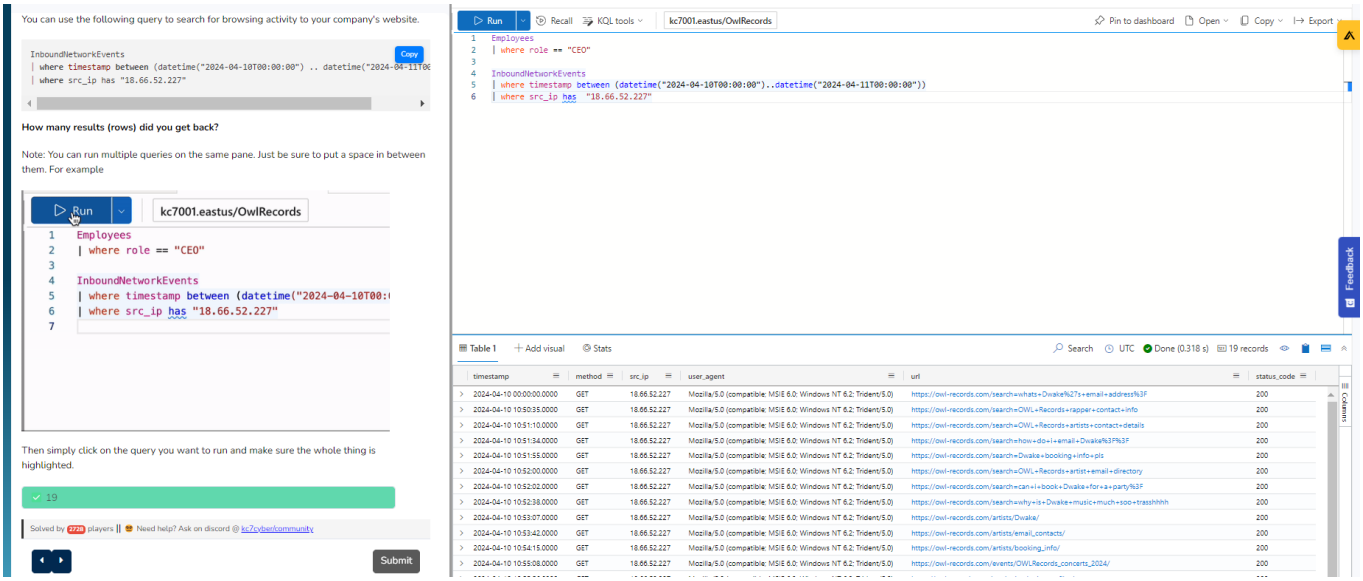


Table 1
Add visual
Stats
Search
UTC
Done (0.160 s)
1 records
hire_date
name
user_agent
ip_addr
email_addr
company_domain
username
role
hostname
2021-05-06 00:00:00.0000
Sean Crater
Mozilla/5.0 (Windows NT 6.3; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0
10.10.0.2
sean_crater@owl-records.com
owl-records.com
secrater
CEO
VMDR-LAPTOP


Enough beef for a burger
Question 4: (10) points
At this point, we'll start digging into the company's data to find clues that will help us solve the mysteries at hand.
We'll use KQL (Kusto Query Language) queries to manipulate our data. Don't worry, we'll provide all the queries in this game, so you don't need to learn how to write them yourself... yet.
For each query we provide, you can simply copy and paste it into the query pane on the right, and then click run. You can use the control-v shortcut to paste.
Run
Recall
KQL tools
kc7001.eastus/OwlRec
Let's take this for a spin. The following query searches for all information about the CEO of OWL Records.
Employees
| where role == "CEO"
Copy
What is the name of the OWL Records CEO?
Sean Crater
Solved by 3054 players || Need help? Ask on discord @ kc7cybercommunity
Submit
kc7001.eastus
kc7001.eastus.OwlR...
kc7001.eastus/OwlRecords
Pin to dashboard
Open
Copy
Export
Feedback
Table 1
Add visual
Stats
Search
UTC
Done (0.160 s)
1 records
hire_date
name
user_agent
ip_addr
email_addr
company_domain
username
role
hostname
2021-05-06 00:00:00.0000
Sean Crater
Mozilla/5.0 (Windows NT 6.3; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0
10.10.0.2
sean_crater@owl-records.com
owl-records.com
secrater
CEO
VMDR-LAPTOP
JPath: /hire_date
Inline
Full
{
"hire_date": 2021-05-06T00:00:00Z,
"name": Sean Crater,
"user_agent": Mozilla/5.0 (Windows NT 6.3; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0,
"ip_addr": 10.10.0.2,
"email_addr": sean_crater@owl-records.com,
"company_domain": owl-records.com,
"username": secrater,
"role": CEO,
"hostname": VMDR-LAPTOP
}


You can use the following query to search for browsing activity to your company's website.
InboundNetworkEvents
| where timestamp between (datetime("2024-04-10T00:00:00") .. datetime("2024-04-11T0
| where src_ip has "18.66.52.227"
Copy
How many results (rows) did you get back?
Note: You can run multiple queries on the same pane. Just be sure to put a space in between them. For example
Run
kc7001.eastus/OwlRecords
1 Employees
2 | where role == "CEO"
3
4 InboundNetworkEvents
5 | where timestamp between (datetime("2024-04-10T00:
6 | where src_ip has "18.66.52.227"
7
Then simply click on the query you want to run and make sure the whole thing is highlighted.
19
Solved by 2728 players || Need help? Ask on discord @ kc7cybercommunity
Submit
Run
Recall
KQL tools
kc7001.eastus/OwlRecords
Pin to dashboard
Open
Copy
Export
1 Employees
2 | where role == "CEO"
3
4 InboundNetworkEvents
5 | where timestamp between (datetime("2024-04-10T00:00:00")..datetime("2024-04-11T00:00:00"))
6 | where src_ip has "18.66.52.227"
Feedback
Table 1
Add visual
Stats
Search
UTC
Done (0.318 s)
19 records
timestamp
method
src_ip
user_agent
url
status_code
2024-04-10 00:00:00.0000 GET 18.66.52.227 Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0) https://owl-records.com/search=whats+Dwake%27s+email+address%3F 200
2024-04-10 10:50:35.0000 GET 18.66.52.227 Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0) https://owl-records.com/search=OWL+Records+rapper+contact+info 200
2024-04-10 10:51:10.0000 GET 18.66.52.227 Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0) https://owl-records.com/search=OWL+Records+artists+contact+details 200
2024-04-10 10:51:34.0000 GET 18.66.52.227 Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0) https://owl-records.com/search=how+do+I+email+Dwake%3F%3F 200
2024-04-10 10:51:55.0000 GET 18.66.52.227 Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0) https://owl-records.com/search=Dwake+booking+info+pls 200
2024-04-10 10:52:00.0000 GET 18.66.52.227 Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0) https://owl-records.com/search=OWL+Records+artist+email+directory 200
2024-04-10 10:52:02.0000 GET 18.66.52.227 Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0) https://owl-records.com/search=can+I+book+Dwake+for+a+party%3F 200
2024-04-10 10:52:38.0000 GET 18.66.52.227 Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0) https://owl-records.com/search=why+is+Dwake+music+much+soo+trasshhhh 200
2024-04-10 10:53:07.0000 GET 18.66.52.227 Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0) https://owl-records.com/artists/Dwake/ 200
2024-04-10 10:53:42.0000 GET 18.66.52.227 Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0) https://owl-records.com/artists/email_contacts/ 200
2024-04-10 10:54:15.0000 GET 18.66.52.227 Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0) https://owl-records.com/artists/booking_info/ 200
2024-04-10 10:55:08.0000 GET 18.66.52.227 Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0) https://owl-records.com/events/OWLRecords_concerts_2024/ 200

Enough beef for a burger — Question 6 (solved): (30) points

The results you are looking at represent someone browsing and searching for information on OWL Records' website.

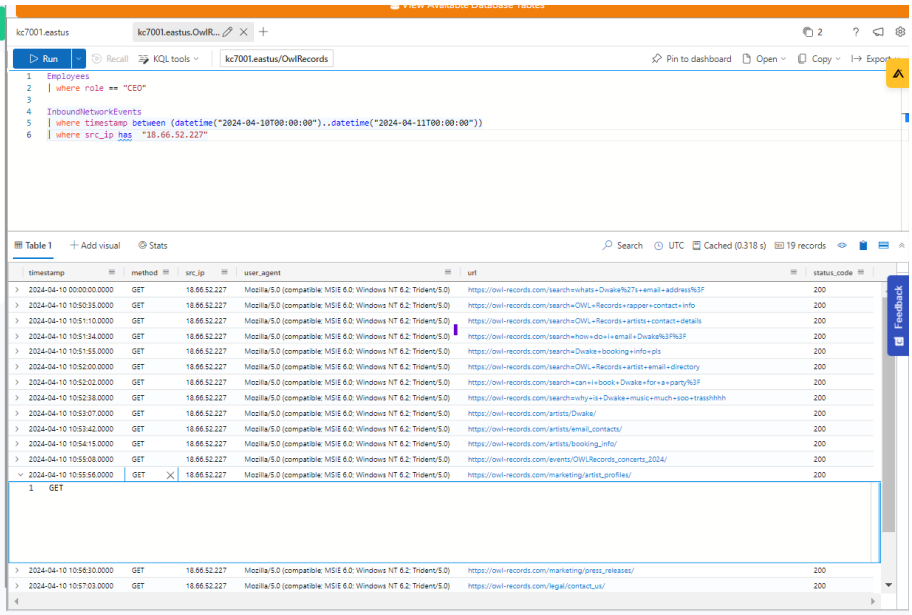
This operator (person browsing the website) was clearly looking to find information about various artists who work for OWL Records, especially Dwake. Thanks to the homie, it looks like we are on the right path.

What piece of information were they looking to get for Dwake? (two words)

email address: email

Solved by 2389 players || Need help? Ask on discord @ kc7cyberlcommunity

Submit



Enough beef for a burger — Question 7 (solved): (30) points

Let's continue to look at the results from the previous query.

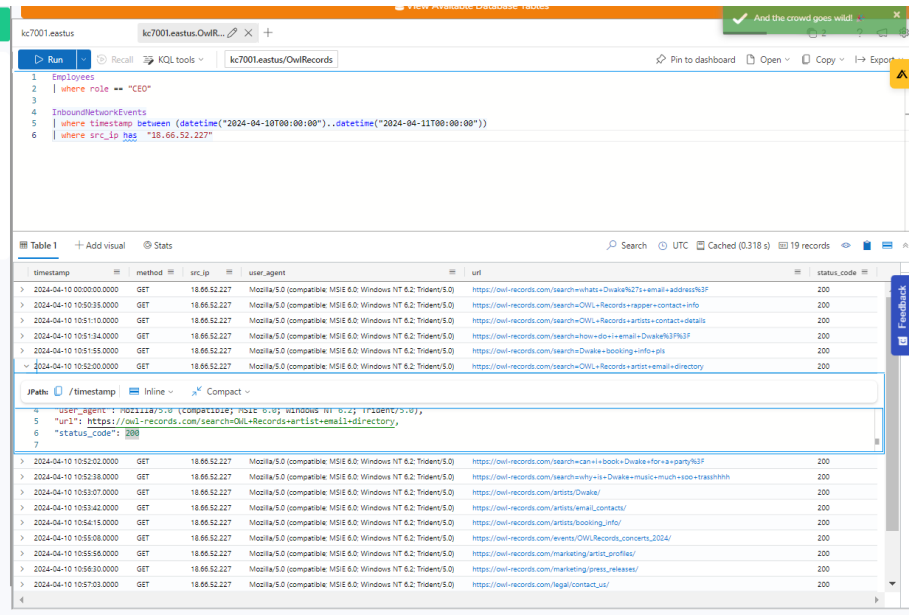
The operator here also expressed their strong opinions about Dwake's music.

The operator is wondering why Dwake's music is so _

trash;trasshhhh

Solved by 2340 players || Need help? Ask on discord @ kc7cyberlcommunity

Submit



Enough beef for a burger — Question 8 (solved): (30) points

Let's continue to look at these logs. At some point the operator discovered Dwake's email address.

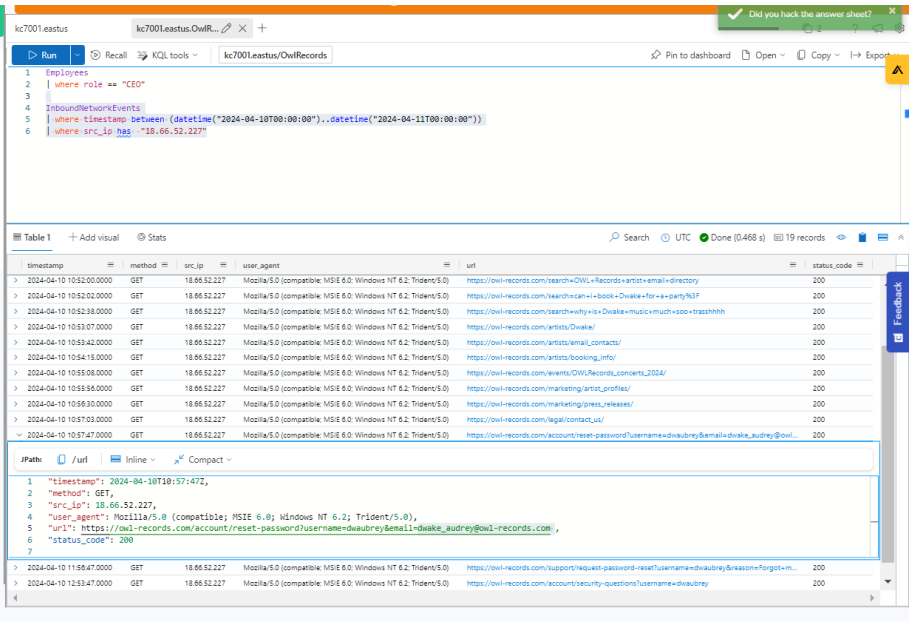
What is Dwake's email address?

You can look at the results from the previous query to find it!

dwake_audrey@owl-records.com

Solved by 2267 players || Need help? Ask on discord @ kc7cyberlcommunity

Submit



Enough beef for a burger Question 9 (solved): (50) points

The operator then attempted to take over Dwake's account by resetting his password. We know this because of the `reset-password` parameter in that last `url` they accessed.

When employees at OWL records need to reset their passwords, they must answer a set of challenge questions to prove who they are. These are the challenge questions offered on the OWL records website:

1. What is your mother's maiden name?
2. What street did you grow up on as a child?
3. What is your childhood pet's name?
4. What is the color of your first car?

Holy smokes! It looks like Dwake may have inadvertently disclosed some of this information in his last verse.

Yo, Present, you don't know where I'm from,
Got the Washington name from my mom's side, son.
It makes sense why they call you present
Cause you're so easy to beat, its pretty much a gift

Used to play with little Fluffy, now I'm runnin' with the wolves,
You say you're on top, but I'm breakin' all the rules.
I'm on that next level, you're stuck in the past,
with those weak beats you won't last.

Which of the following did Dwake disclose in his verse? (pick one)

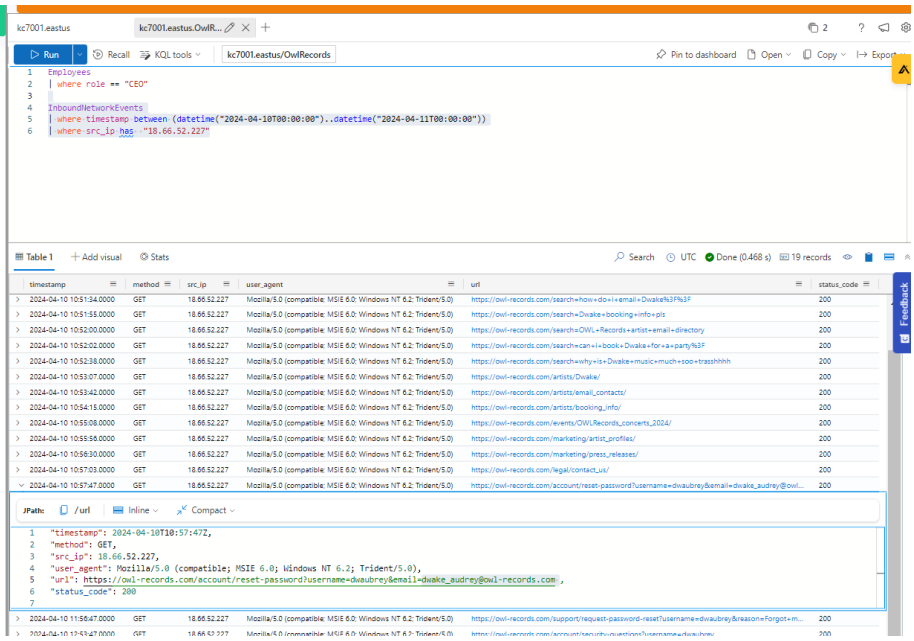
1 and 2
2 and 3
1 and 3
2 and 4

Copy

✓ 1 and 3

Solved by 2233 players || Need help? Ask on discord @ kc7cybercommunity

Submit



Enough beef for a burger Question 10 (solved): (50) points

Looking at the verse, let's try to figure out what values the operator may have tried to use to reset Dwake's password.

Yo, Present, you don't know where I'm from,
Got the Washington name from my mom's side, son.
It makes sense why they call you present
Cause you're so easy to beat, its pretty much a gift

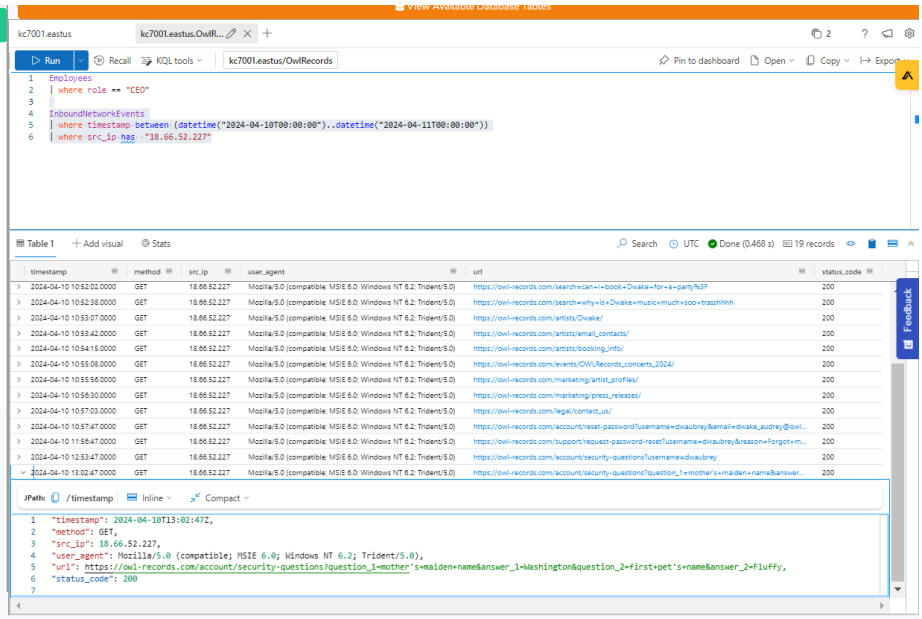
Used to play with little Fluffy, now I'm runnin' with the wolves,
You say you're on top, but I'm breakin' all the rules.
I'm on that next level, you're stuck in the past,
with those weak beats you won't last.

What is Dwake's mother's maiden name?

✓ Washington

Solved by 2190 players || Need help? Ask on discord @ kc7cybercommunity

Submit



Enough beef for a burger — Question 11 (solved): (50) points

Dwake also reveals the name of his childhood pet

Yo, Present, you don't know where I'm from,
Got the Washington name from my mom's side, son.
It makes sense why they call you present
Cause you're so easy to beat, its pretty much a gift

Used to play with little Fluffy, now I'm runnin' with the wolves,
You say you're on top, but I'm breakin' all the rules.
I'm on that next level, you're stuck in the past,
with those weak beats you won't last.

What is the name of Dwake's childhood pet?

Fluffy

Solved by 7196 players || Need help? Ask on discord @ kc7cyber/community

Submit

I'm not worthy!

kc7001.eastus | kc7001.eastus.OwlR... | kc7001.eastus/OwlRecords

Run | Recall | KQL tools | Pin to dashboard | Open | Copy | Export

```
Employees
| where role == "CEO"

InboundNetworkEvents
| where timestamp between (datetime("2024-04-10T00:00:00")..datetime("2024-04-11T00:00:00"))
| where src_ip has "18.66.52.227"
```

Table 1 | Add visual | Stats | Search | UTC | Done (0.468 s) | 19 records

timestamp	method	src_ip	user_agent	url	status_code
2024-04-10 10:52:02.0000	GET	18.66.52.227	Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0)	https://owl-records.com/search=can+i+book+Dwake+for+a+party%3F	200
2024-04-10 10:52:38.0000	GET	18.66.52.227	Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0)	https://owl-records.com/search=why+is+Dwake+music+much+soo+trashhhhh	200
2024-04-10 10:53:07.0000	GET	18.66.52.227	Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0)	https://owl-records.com/artists/Dwake/	200
2024-04-10 10:53:42.0000	GET	18.66.52.227	Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0)	https://owl-records.com/artists/email_contacts/	200
2024-04-10 10:54:15.0000	GET	18.66.52.227	Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0)	https://owl-records.com/artists/booking_info/	200
2024-04-10 10:55:08.0000	GET	18.66.52.227	Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0)	https://owl-records.com/events/OWLRecords_concerts_2024/	200
2024-04-10 10:55:56.0000	GET	18.66.52.227	Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0)	https://owl-records.com/marketing/artist_profiles/	200
2024-04-10 10:56:30.0000	GET	18.66.52.227	Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0)	https://owl-records.com/marketing/press_releases/	200
2024-04-10 10:57:03.0000	GET	18.66.52.227	Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0)	https://owl-records.com/legal/contact_us/	200
2024-04-10 10:57:47.0000	GET	18.66.52.227	Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0)	https://owl-records.com/account/reset-password?username=dwaubrey&email=dwake_audrey@owl...	200
2024-04-10 11:56:47.0000	GET	18.66.52.227	Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0)	https://owl-records.com/support/request-password-reset?username=dwaubrey&reason=Forgot+m...	200
2024-04-10 12:53:47.0000	GET	18.66.52.227	Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0)	https://owl-records.com/account/security-questions?username=dwaubrey	200
2024-04-10 13:02:47.0000	GET	18.66.52.227	Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0)	https://owl-records.com/account/security-questions?question_1=mother's+maiden+name&answer...	200

JPath: /timestamp | Inline | Compact


```
{
"timestamp": 2024-04-10T13:02:47Z,
"method": GET,
"src_ip": 18.66.52.227,
"user_agent": Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0),
"url": https://owl-records.com/account/security-questions?question_1=mother's+maiden+name&answer_1=Washington&question_2=first+pet's+name&answer_2=Fluffy,
"status_code": 200
}
```


Feedback

Less beef, more phish — Question 4 (solved): (50) points

Woohoo! We have a domain name! Things will be a lot smoother from here on out! Let's look in email logs for evidence that this domain was used.

First we'll take a quick gander at the email logs. We can use the `take` operator to look at ten random rows.

```
Email
| take 10
```

Copy

Which column in the email table is most likely to contain our domain?

link

Solved by 6943 players || Need help? Ask on discord @ kc7cyber/community

Submit

Close, but no cigar!

It's in!

kc7001.eastus | kc7001.eastus.OwlR... | kc7001.eastus/OwlRecords

Run | Recall | KQL tools | Pin to dashboard | Copy | Export

```
Email
| take 10
```

Table 1 | Add visual | Stats | Search | UTC | Done (0.999 s) | 10 records

timestamp	sender	reply_to	recipient	subject	verdict	link
2024-04-01 07:44:27.0000	larry_russell@beatmakers-online.com	larry_russell@beatmakers-online.com	greg_wells@owl-records.com	[EXTERNAL] RE:RE: Embarr...	CLEAN	https://drive.google.com/drive/u/...
2024-04-01 07:57:52.0000	chance_west@owl-records.com	chance_west@owl-records.com	lil_zee@owl-records.com	FW: Also respect use web ...		https://docs.google.com/spreadsh...
2024-04-01 08:15:22.0000	joseph_johnson@owl-records.com	joseph_johnson@owl-records.com	christine_baran@beatmakers-online.com	The the conflict the the of ...		https://docs.google.com/spreadsh...
2024-04-01 08:36:14.0000	lauri_lawrence@owl-records.com	lauri_lawrence@owl-records.com	megannguyen@yahoo.com	Rake conflict his grew an p...		https://images.owl-records.com/st...
2024-04-01 08:55:48.0000	samuel_manson@beatmakers-online.com	samuel_manson@beatmakers-online.com	benny_nixon@owl-records.com	[EXTERNAL] FW: New sever...	CLEAN	https://kcfoundation.org/public/sh...
2024-04-01 09:21:46.0000	matrilineal.windowshopping@aol.com	matrilineal.windowshopping@aol.com	mariah_hart@owl-records.com	[EXTERNAL] For malicious ...	SUSPICIOUS	https://nodehill.se/share/publishe...
2024-04-01 09:44:58.0000	william_farnham@owl-records.com	william_farnham@owl-records.com	luella_zullo@owl-records.com	From conflict era stirring le...		http://graph-fast.fastly.net/7QfHBh
2024-04-01 10:06:41.0000	logic_white@owl-records.com	logic_white@owl-records.com	leahclark@gmail.com	FW: Present business and r...		https://owl-records.sharepoint.co...
2024-04-01 10:15:22.0000	quincy_carter@owl-records.com	quincy_carter@owl-records.com	oneida_lampron@owl-records.com	RE: Details truce the inform...		https://47557.akamaiedge.net
2024-04-01 10:19:58.0000	henrywright@protonmail.com	henrywright@protonmail.com	armando_hunley@owl-records.com	[EXTERNAL] Web label era ...	BLOCKED	http://JXJ8H0F4M6.cloudfront.net

JPath: /timestamp | Inline | Compact


```
{
"timestamp": 2024-04-01T10:19:58Z,
"sender": henrywright@protonmail.com,
"reply_to": henrywright@protonmail.com,
"recipient": armando_hunley@owl-records.com,
"subject": [EXTERNAL] Web label era on successful track web track the on,
"verdict": BLOCKED,
"link": http://JXJ8H0F4M6.cloudfront.net
}
```


Less beef, more phish — Question 5 (solved): (30) points

Great now let's look for the domain in that column.

```
Email
| where link has "betterlyrics4u.com"
```

Copy

How many results did we get from this query?

13

Solved by 5974 players || Need help? Ask on discord @ kc7cyber/community

Submit

CORRECT!!!

kc7001.eastus | kc7001.eastus.OwlR... | kc7001.eastus/OwlRecords

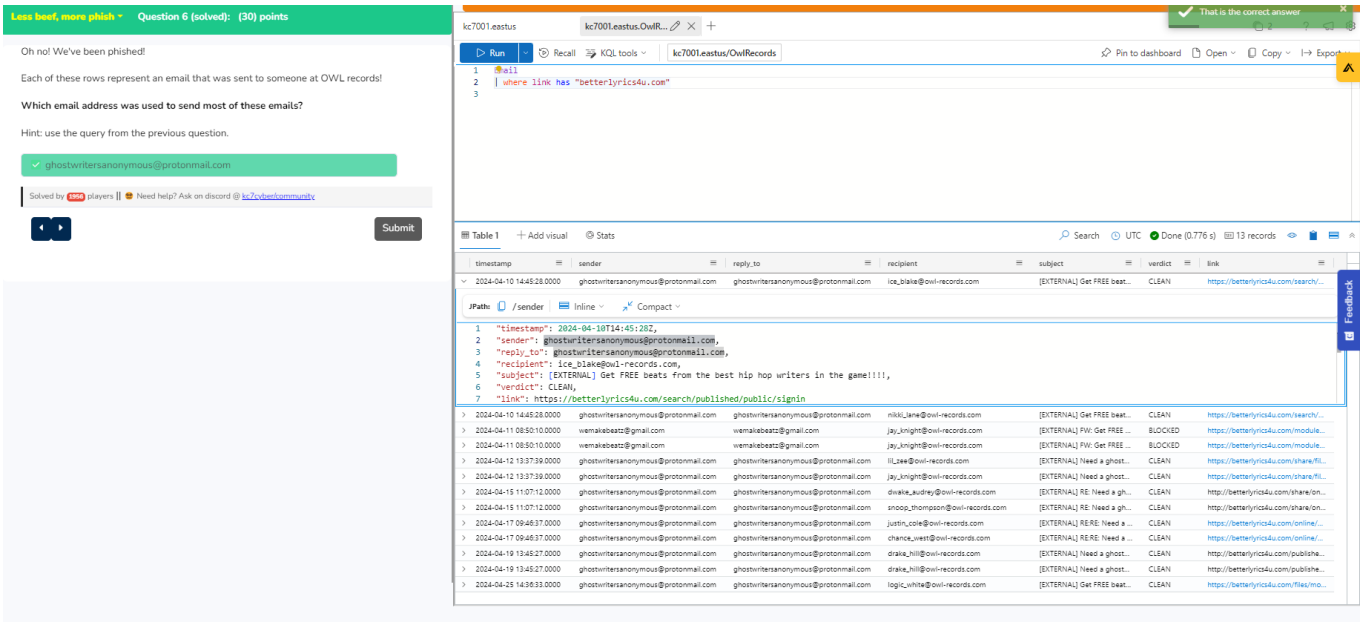
Run | Recall | KQL tools | Pin to dashboard | Open | Copy | Export

```
Email
| where link has "betterlyrics4u.com"
```

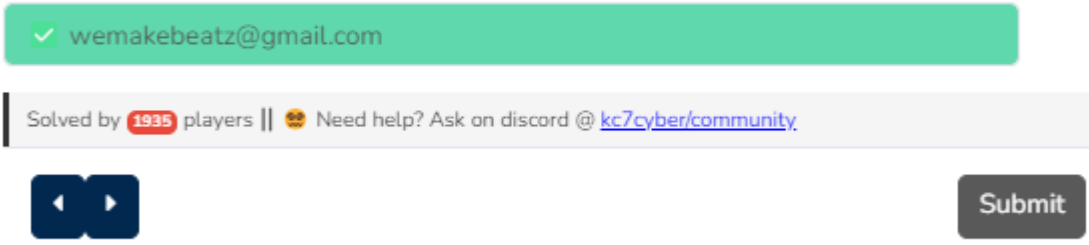
Table 1 | Add visual | Stats | Search | UTC | Done (0.776 s) | 13 records

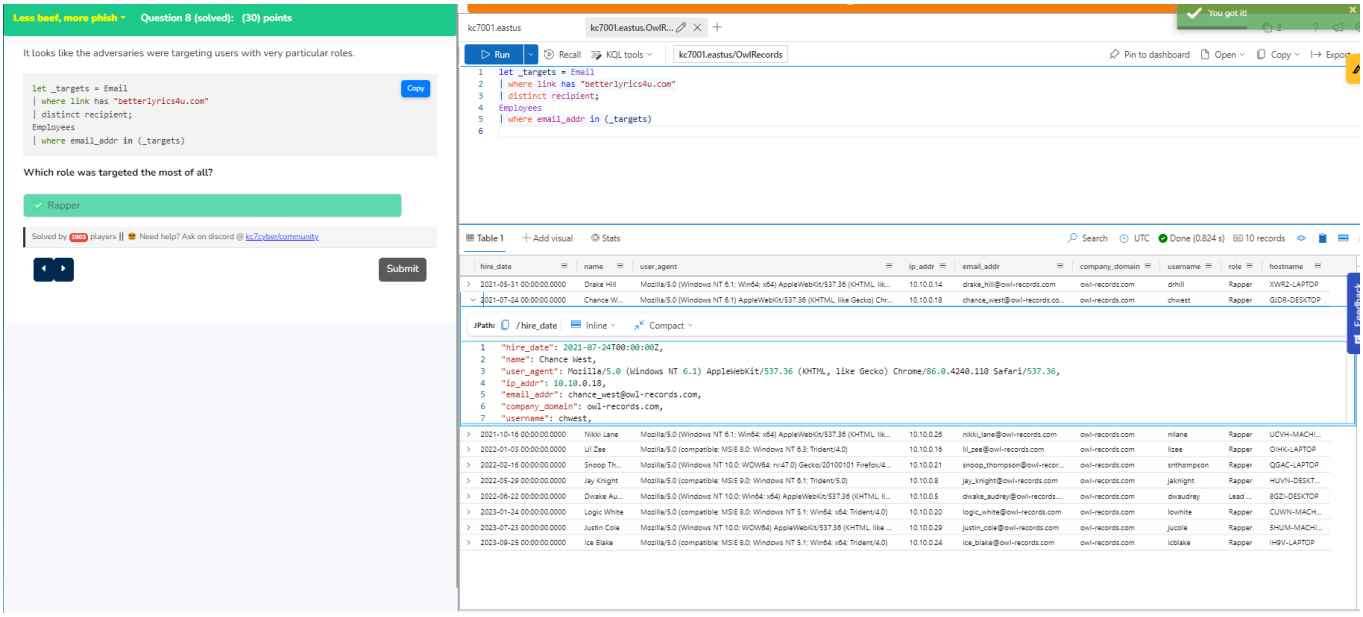
timestamp	sender	reply_to	recipient	subject	verdict	link
2024-04-10 14:45:28.0000	ghostwritersanonymous@protonmail.com	ghostwritersanonymous@protonmail.com	ice_blake@owl-records.com	[EXTERNAL] Get FREE beat...	CLEAN	https://betterlyrics4u.com/search/...
2024-04-10 14:45:28.0000	ghostwritersanonymous@protonmail.com	ghostwritersanonymous@protonmail.com	nikki_lane@owl-records.com	[EXTERNAL] Get FREE beat...	CLEAN	https://betterlyrics4u.com/search/...
2024-04-11 08:50:10.0000	wemakebeatz@gmail.com	wemakebeatz@gmail.com	jay_knight@owl-records.com	[EXTERNAL] FW: Get FREE ...	BLOCKED	https://betterlyrics4u.com/module...
2024-04-11 08:50:10.0000	wemakebeatz@gmail.com	wemakebeatz@gmail.com	jay_knight@owl-records.com	[EXTERNAL] FW: Get FREE ...	BLOCKED	https://betterlyrics4u.com/module...
2024-04-12 13:37:39.0000	ghostwritersanonymous@protonmail.com	ghostwritersanonymous@protonmail.com	lil_zee@owl-records.com	[EXTERNAL] Need a ghost...	CLEAN	https://betterlyrics4u.com/share/fil...
2024-04-12 13:37:39.0000	ghostwritersanonymous@protonmail.com	ghostwritersanonymous@protonmail.com	jay_knight@owl-records.com	[EXTERNAL] Need a ghost...	CLEAN	https://betterlyrics4u.com/share/fil...
2024-04-15 11:07:12.0000	ghostwritersanonymous@protonmail.com	ghostwritersanonymous@protonmail.com	dwake_audrey@owl-records.com	[EXTERNAL] RE: Need a gh...	CLEAN	http://betterlyrics4u.com/share/on...
2024-04-15 11:07:12.0000	ghostwritersanonymous@protonmail.com	ghostwritersanonymous@protonmail.com	snoop_thompson@owl-records.com	[EXTERNAL] RE: Need a gh...	CLEAN	http://betterlyrics4u.com/share/on...
2024-04-17 09:46:37.0000	ghostwritersanonymous@protonmail.com	ghostwritersanonymous@protonmail.com	justin_cole@owl-records.com	[EXTERNAL] RE:RE: Need a ...	CLEAN	https://betterlyrics4u.com/online/...
2024-04-17 09:46:37.0000	ghostwritersanonymous@protonmail.com	ghostwritersanonymous@protonmail.com	chance_west@owl-records.com	[EXTERNAL] RE:RE: Need a ...	CLEAN	https://betterlyrics4u.com/online/...
2024-04-19 13:45:27.0000	ghostwritersanonymous@protonmail.com	ghostwritersanonymous@protonmail.com	drake_hill@owl-records.com	[EXTERNAL] Need a ghost...	CLEAN	http://betterlyrics4u.com/publishe...
2024-04-19 13:45:27.0000	ghostwritersanonymous@protonmail.com	ghostwritersanonymous@protonmail.com	drake_hill@owl-records.com	[EXTERNAL] Need a ghost...	CLEAN	http://betterlyrics4u.com/publishe...
2024-04-25 14:36:33.0000	ghostwritersanonymous@protonmail.com	ghostwritersanonymous@protonmail.com	logic_white@owl-records.com	[EXTERNAL] Get FREE beat...	CLEAN	https://betterlyrics4u.com/files/mo...

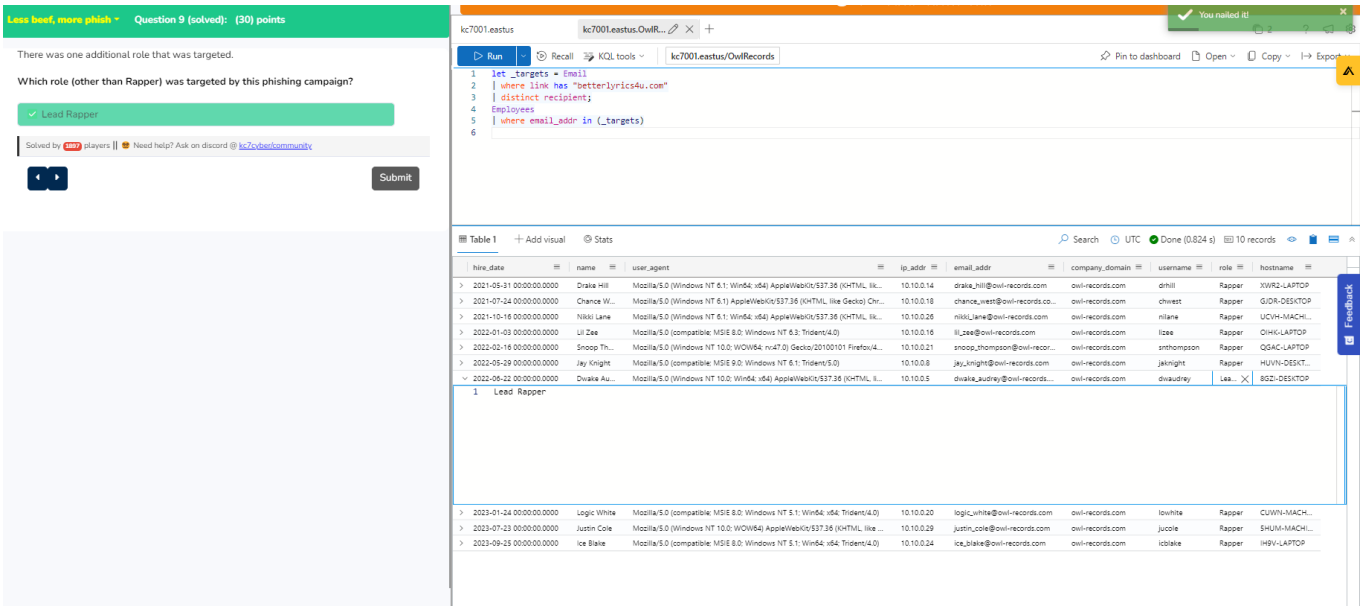
Feedback

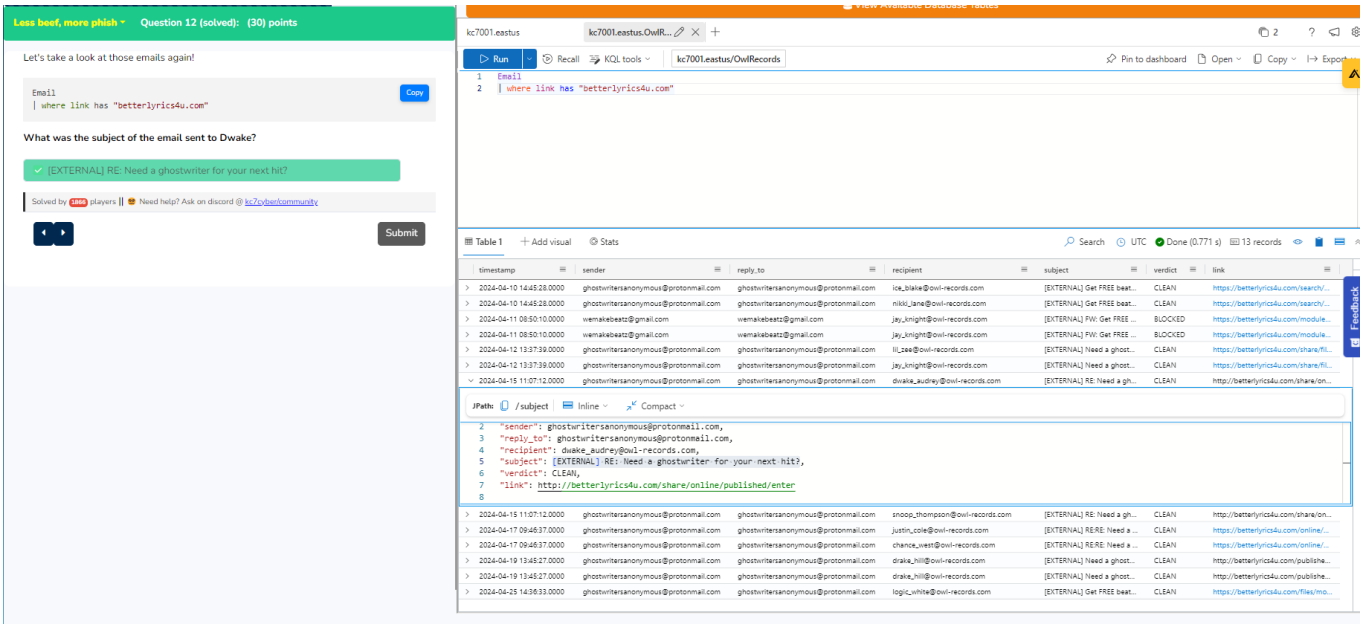


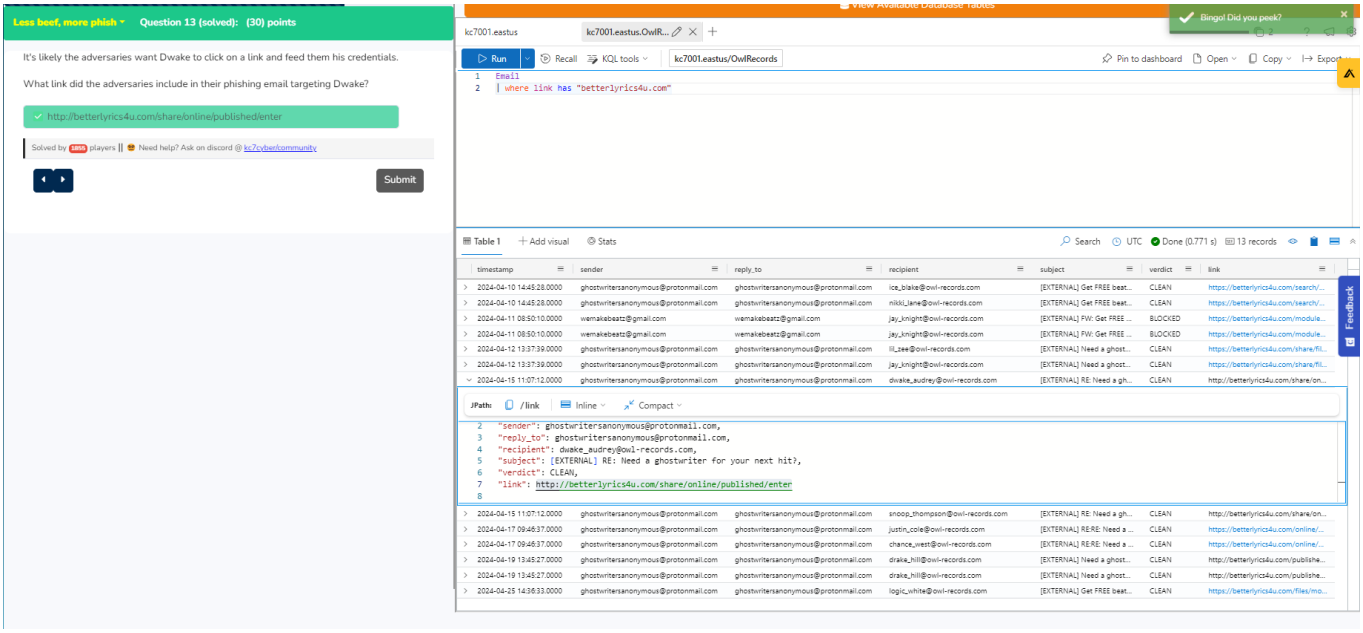
What was the other email address used to send these phishing emails?






Less beef, more phish
Question 9 (solved): (30) points
There was one additional role that was targeted.
Which role (other than Rapper) was targeted by this phishing campaign?
Lead Rapper
Solved by 1867 players || Need help? Ask on discord @ kc7cyber/community
Submit
You nailed it!
kc7001.eastus
kc7001.eastus.OwlR...
Run
Recall
KQL tools
kc7001.eastus/OwlRecords
Pin to dashboard
Open
Copy
Export
let _targets = Email
| where link has "betterlyrics4u.com"
| distinct recipient;
Employees
| where email_addr in (_targets)
Table 1
Add visual
Stats
Search
UTC
Done (0.824 s)
10 records
hire_date
name
user_agent
ip_addr
email_addr
company_domain
username
role
hostname
Lead Rapper
Feedback


Less beef, more phish
Question 12 (solved): (30) points
Let's take a look at those emails again!
Email
| where link has "betterlyrics4u.com"
Copy
What was the subject of the email sent to Dwake?
[EXTERNAL] RE: Need a ghostwriter for your next hit?
Solved by 1866 players || Need help? Ask on discord @ kc7cyber/community
Submit
kc7001.eastus
kc7001.eastus.OwlR...
Run
Recall
KQL tools
kc7001.eastus/OwlRecords
Pin to dashboard
Open
Copy
Export
Email
| where link has "betterlyrics4u.com"
Table 1
Add visual
Stats
Search
UTC
Done (0.771 s)
13 records
timestamp
sender
reply_to
recipient
subject
verdict
link
JPath
/subject
Inline
Compact
"sender": ghostwritersanonymous@protonmail.com,
"reply_to": ghostwritersanonymous@protonmail.com,
"recipient": dwake_audrey@owl-records.com,
"subject": [EXTERNAL] RE: Need a ghostwriter for your next hit?,
"verdict": CLEAN,
"link": http://betterlyrics4u.com/share/online/published/enter
Feedback


Less beef, more phish
Question 13 (solved): (30) points
It's likely the adversaries want Dwake to click on a link and feed them his credentials.
What link did the adversaries include in their phishing email targeting Dwake?
http://betterlyrics4u.com/share/online/published/enter
Solved by 1858 players || Need help? Ask on discord @ kc7cyber/community
Submit
Bingo! Did you peek?
kc7001.eastus
kc7001.eastus.OwlR...
Run
Recall
KQL tools
kc7001.eastus/OwlRecords
Pin to dashboard
Open
Copy
Export
Email
| where link has "betterlyrics4u.com"
Table 1
Add visual
Stats
Search
UTC
Done (0.771 s)
13 records
timestamp
sender
reply_to
recipient
subject
verdict
link
JPath
/link
Inline
Compact
"sender": ghostwritersanonymous@protonmail.com,
"reply_to": ghostwritersanonymous@protonmail.com,
"recipient": dwake_audrey@owl-records.com,
"subject": [EXTERNAL] RE: Need a ghostwriter for your next hit?,
"verdict": CLEAN,
"link": http://betterlyrics4u.com/share/online/published/enter
Feedback

Less beef, more phish — Question 14: (30) points

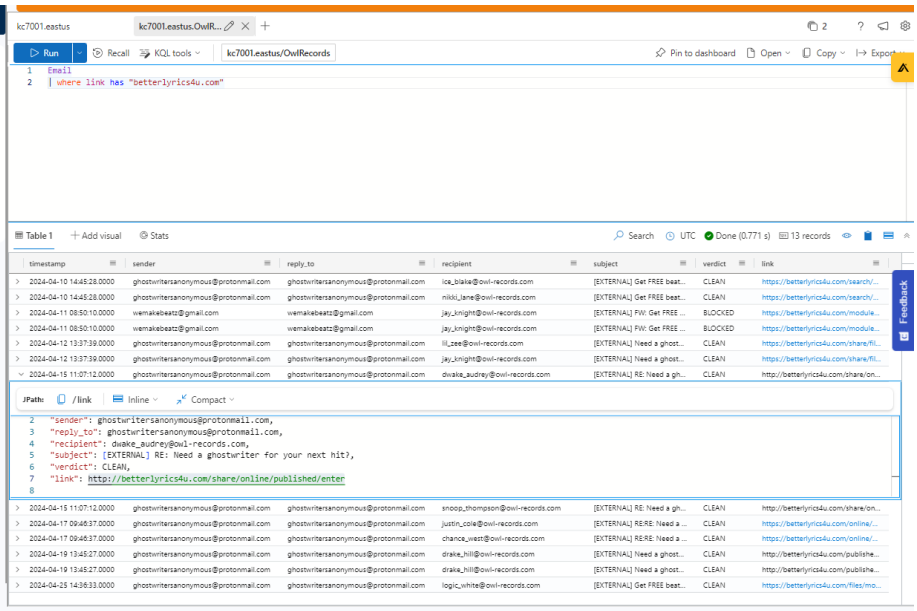
On occasion, our email security product will block suspicious email. In those cases, the end users will never even see the suspicious emails.

What was the verdict of the email sent to Dwake?

CLEAN

Solved by 1851 players || Need help? Ask on discord @ kc7cyberlcommunity

Submit



Less beef, more phish — Question 15 (solved): (10) points

Here is the phishing email Dwake was presented with.

That's pretty convincing.

[EXTERNAL] RE: Need a ghostwriter for your next hit?

Inbox ×

Ghost Writer 9:35 PM (5 hours ago)

to me

Hi Dwake,

I've heard you're looking for a ghostwriter to help with your next hit song. I'm a professional writer with a track record of creating chart-toppers. Let's discuss how we can collaborate.

Please find attached my portfolio and let's set up a call to discuss further. I'm excited about the opportunity to work with you.

Click here to login and schedule a meeting with me

Best,
GhostWriter

What name (or nickname) did the aversaries sign the email with?

ghostwriter

Solved by 1850 players || Need help? Ask on discord @ kc7cyberlcommunity

Submit