

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

Solved by **3766** players || 🤖 Need help? Ask on discord @ [kc7cyber/community](https://discord.com/invite/kc7cyber/community)



Submit

kc7001.eastus

Run Recall KQL tools kc7001.eastus/OwlRecords

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

Pin to dashboard Open Copy Export

| 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 |

Table 1 Add visual Stats Search UTC Done (0.160 s) 1 records

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 **Ctrl+V** shortcut to paste.

Run Recall KQL tools kc7001.eastus/OwlRecords

```
1
```

Let's take this for a spin. The following query searches for all information about the CEO of OWL Records.

Employees
| where role == "CEO"

What is the name of the OWL Records CEO?

Sean Crater

Solved by 1004 players | Need help? Ask on discord @ [k7vds/commu](#)

Submit

kc7001.eastus

Run Recall KQL tools kc7001.eastus/OwlRecords

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

Pin to dashboard Open Copy Export

| 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 |

Table 1 Add visual Stats Search UTC Done (0.160 s) 1 records

Path: /hire_date Inline Full

```
1 "hire_date": 2021-05-06T00:00:00Z,
2 "name": Sean Crater,
3 "user_agent": Mozilla/5.0 (Windows NT 6.3; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0,
4 "ip_addr": 10.10.0.2,
5 "email_addr": sean_crater@owl-records.com,
6 "company_domain": owl-records.com,
7 "username": secrater,
8 "role": CEO,
9 "hostname": VMDR-LAPTOP
10
```

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("2024-04-11T00:00:00")
| where src_ip has "18.66.52.227"
```

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 between them. For example

Run Recall KQL tools kc7001.eastus/OwlRecords

```
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"
7
```

Then simply click on the query you want to run and make sure the whole thing is highlighted.

19

Solved by 629 players | Need help? Ask on discord @ [k7vds/commu](#)

Submit

Run Recall KQL tools kc7001.eastus/OwlRecords

```
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"
```

Pin to dashboard Open Copy Export

| 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+shato+Dvalke%27+email+address%3F | 200 |
| 2024-04-10 10:50:38.0000 | GET | 18.66.52.227 | Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0) | https://owl-records.com/search+Dvalke+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+how+de+email+Dvalke%3F%3F | 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+de+email+Dvalke%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+can+i+book+music+for+a+party%3F | 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+music+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+can+i+book+music+for+a+party%3F | 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/search+can+i+book+music+for+a+party%3F | 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/search+can+i+book+music+for+a+party%3F | 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/search+can+i+book+music+for+a+party%3F | 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/search+can+i+book+music+for+a+party%3F | 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 1025 players • Need help? Ask on discord @ [kc7yabcommunity](#)

Submit

kc7001.eastus

Run Recall KQL tools kc7001.eastus/OwlRecords

```
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"
```

Table 1 + Add visual Stats Search UTC Cached (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=what+Dwake%27+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+artist+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 10:51:53.0000 | 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 10:52:02.0000 | 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+i+Dwake+music+much+soo+trashhhh | 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/OWLRecordsconcerts_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 |

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 _

✓ trashtrashhhh

Solved by 1025 players • Need help? Ask on discord @ [kc7yabcommunity](#)

Submit

kc7001.eastus

Run Recall KQL tools kc7001.eastus/OwlRecords

```
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"
```

Table 1 + Add visual Stats Search UTC Cached (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=what+Dwake%27+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+artist+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 10:51:53.0000 | 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 10:52:02.0000 | GET | 18.66.52.227 | Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0) | https://owl-records.com/search=OWL+Records+artist+email+directory | 200 |

KQL Query:

```
1 user_agent: Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0);
2 url: https://owl-records.com/search=OWL-Records+artist+email+directory,
3 status_code: 200
```

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 1025 players • Need help? Ask on discord @ [kc7yabcommunity](#)

Submit

kc7001.eastus

Run Recall KQL tools kc7001.eastus/OwlRecords

```
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"
```

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+i+Dwake+music+much+soo+trashhhh | 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/OWLRecordsconcerts_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 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/account/reset-password?username=dwake_audrey&email=dwake_audrey@owl-records.com | 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/support/request-password-reset?username=dwake_audrey&reason=Forgot+m... | 200 |

KQL Query:

```
1 "timestamp": 2024-04-10T10:57:47Z,
2 "method": GET,
3 "src_ip": 18.66.52.227,
4 "user_agent": Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0),
5 "url": https://owl-records.com/account/reset-password?username=dwake_audrey&email=dwake_audrey@owl-records.com,
6 "status_code": 200
```

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 `ip1` 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

Solved by 625 players • Need help? Ask on discord @ [k2xvbsdkcommunity](#)

kc7001.eastus

Run Recall KQL tools kc7001.eastus/OWLRecords

```
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"
```

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 10:51:34.0000 | 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=Dwakeh3P%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+ps | 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=Dwake+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+sco+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/events/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=dwaka_audrey@owl... | 200 |

/Path: /url Inline Compact

```
1 "timestamp": 2024-04-10T10:57:47Z,
2 "method": GET,
3 "src_ip": 18.66.52.227,
4 "user_agent": Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0),
5 "url": https://owl-records.com/account/reset-password?username=dwaubrey&email=dwaka_audrey@owl-records.com,
6 "status_code": 200
7
```

> 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 12:43:47.0000 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

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 610 players • Need help? Ask on discord @ [k2xvbsdkcommunity](#)

kc7001.eastus

Run Recall KQL tools kc7001.eastus/OWLRecords

```
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"
```

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+sco+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/events/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=dwaka_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 12:43:47.0000 | 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 |
| > 2024-08-10 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_1=Washington&question_2=firstpet's+name&answer_2=Fluffy, | 200 |

/Path: /timestamp Inline Compact

```
1 "timestamp": 2024-04-10T13:02:47Z,
2 "method": GET,
3 "src_ip": 18.66.52.227,
4 "user_agent": Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0),
5 "url": https://owl-records.com/account/security-questions?question_1=mother's+maiden+name&answer_1=Washington&question_2=firstpet's+name&answer_2=Fluffy,
6 "status_code": 200
7
```

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

Dwawe 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, it's 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 Dwawe's childhood pet?

✓ Fluffy

Solved by 100+ players || Need help? Ask on discord @ [k2cybercommunity](#)

Submit

kc7001.eastus

Run Recall KQL tools kc7001.eastus/OwlRecords

```
1 Employees
2 | where role == "CEO"
3
4 InboundNetworkEvents
5 | where timestamp between (datetime("2024-04-10T08:00:00"), datetime("2024-04-11T08:00:00"))
6 | 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+Dwawe+for+a+party&P | 200 |
| 2024-04-10 10:52:26.0000 | 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+Dwawe+music+much+easier+to+stashttttt | 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/Dwawe/ | 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 10:54:16.0000 | 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 10:55:58.0000 | 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 10:56:22.0000 | 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 10:56:30.0000 | 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/account/reset-password?username=dwawe&email=dwawe_audrey@owl... | 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/support/request-password-reset?username=dwawe&reason=Forgot+m... | 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/account/security-questions?username=dwawe&... | 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=maiden+name&answer_2=Fluffy, | 200 |

JPath: /timestamp Inline Compact

```
1 "timestamp": 2024-04-10T13:02:47Z,
2 "method": GET,
3 "src_ip": 18.66.52.227,
4 "user_agent": Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.2; Trident/5.0),
5 "url": https://owl-records.com/account/security-questions?question_1=maiden+name&answer_2=Fluffy,
6 "status_code": 200
7
```

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

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

✓ link

Solved by 100+ players || Need help? Ask on discord @ [k2cybercommunity](#)

Submit

kc7001.eastus

Run Recall KQL tools kc7001.eastus/OwlRecords

```
1 Email
2 | take 10
3
```

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_jussel@beetmakers-online.com | larry_jussel@beetmakers-online.com | greg_wells@owl-records.com | [EXTERNAL] RE:RE Embarr... | CLEAN | https://drive.google.com/drive/v... |
| 2024-04-01 07:57:52.0000 | chance_west@owl-records.com | chance_west@owl-records.com | ilLse@owl-records.com | FW: Also respect web use... | | https://docs.google.com/spreads... |
| 2024-04-01 08:16:22.0000 | joseph_johnson@owl-records.com | joseph_johnson@owl-records.com | christine_baran@beetmakers-online.com | The the conflict the of... | | https://images.owl-records.com/st... |
| 2024-04-01 08:36:14.0000 | lauri_lawrence@owl-records.com | lauri_lawrence@owl-records.com | megan_guyen@yahoo.com | Rale conflict his grew an p... | | https://kctfs.vodafone.org/public/sh... |
| 2024-04-01 09:55:48.0000 | samuel_manson@beetmakers-online.com | samuel_manson@beetmakers-online.com | benmy_johnson@owl-records.com | [EXTERNAL] FW: New sever... | CLEAN | https://modestillix.there/publish... |
| 2024-04-01 09:57:45.0000 | martineal.windowshopping@aol.com | martineal.windowshopping@aol.com | mariah_hart@owl-records.com | [EXTERNAL] For malicious ... | SUSPICIOUS | https://modestillix.there/publish... |
| 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 string la... | | https://graph.fastfatty.net/7Qf0sh |
| 2024-04-01 10:06:41.0000 | logic_white@owl-records.com | logic_white@owl-records.com | leahdani@gmail.com | FW: Present business and r... | | https://betterlyrics4u.com/share/on... |
| 2024-04-01 10:16:22.0000 | quincy_carter@owl-records.com | quincy_carter@owl-records.com | onaida_lamerson@owl-records.com | RE: Details track the inform... | | https://a7557.akamaiedge.net |
| 2024-04-01 10:19:58.0000 | henrywright@protonmail.com | henrywright@protonmail.com | amando_hunley@owl-records.com | [EXTERNAL] Web label era on successful track web track the on, | BLOCKED | http://3XJ8H9F4N6.cloudfront.net |

JPath: /timestamp Inline Compact

```
1 "timestamp": 2024-04-01T10:19:58Z,
2 "sender": henrywright@protonmail.com,
3 "reply_to": henrywright@protonmail.com,
4 "recipient": amando_hunley@owl-records.com,
5 "subject": [EXTERNAL] Web label era on successful track web track the on,
6 "verdict": BLOCKED,
7 "link": http://3XJ8H9F4N6.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"

How many results did we get from this query?

✓ 13

Solved by 100+ players || Need help? Ask on discord @ [k2cybercommunity](#)

Submit

kc7001.eastus

Run Recall KQL tools kc7001.eastus/OwlRecords

```
1 Email
2 | where link has "betterlyrics4u.com"
3
```

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 | ghostwriteranonymous@protonmail.com | ghostwriteranonymous@protonmail.com | ica_state@owl-records.com | [EXTERNAL] Get FREE beat... | CLEAN | https://betterlyrics4u.com/search/... |
| 2024-04-10 14:45:28.0000 | ghostwriteranonymous@protonmail.com | ghostwriteranonymous@protonmail.com | nikki_lane@owl-records.com | [EXTERNAL] Get FREE beat... | CLEAN | https://betterlyrics4u.com/search/... |
| 2024-04-11 08:50:10.0000 | wemakebeats@gmail.com | wemakebeats@gmail.com | jay_jnright@owl-records.com | [EXTERNAL] FW: Get FREE ... | BLOCKED | https://betterlyrics4u.com/module... |
| 2024-04-11 08:50:10.0000 | wemakebeats@gmail.com | wemakebeats@gmail.com | jay_jnright@owl-records.com | [EXTERNAL] FW: Get FREE ... | BLOCKED | https://betterlyrics4u.com/module... |
| 2024-04-12 13:37:39.0000 | ghostwriteranonymous@protonmail.com | ghostwriteranonymous@protonmail.com | ilLse@owl-records.com | [EXTERNAL] Need a ghost... | CLEAN | https://betterlyrics4u.com/share/fi... |
| 2024-04-12 13:37:39.0000 | ghostwriteranonymous@protonmail.com | ghostwriteranonymous@protonmail.com | jay_jnright@owl-records.com | [EXTERNAL] Need a ghost... | CLEAN | https://betterlyrics4u.com/share/fi... |
| 2024-04-15 11:07:12.0000 | ghostwriteranonymous@protonmail.com | ghostwriteranonymous@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 | ghostwriteranonymous@protonmail.com | ghostwriteranonymous@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 | ghostwriteranonymous@protonmail.com | ghostwriteranonymous@protonmail.com | justice_cole@owl-records.com | [EXTERNAL] Need a ghost... | CLEAN | https://betterlyrics4u.com/online/... |
| 2024-04-17 09:46:37.0000 | ghostwriteranonymous@protonmail.com | ghostwriteranonymous@protonmail.com | chance_west@owl-records.com | [EXTERNAL] RE:RE: Need a ... | CLEAN | https://betterlyrics4u.com/online/... |
| 2024-04-19 13:45:27.0000 | ghostwriteranonymous@protonmail.com | ghostwriteranonymous@protonmail.com | drake_hill@owl-records.com | [EXTERNAL] Need a ghost... | CLEAN | http://betterlyrics4u.com/publish... |
| 2024-04-19 13:45:27.0000 | ghostwriteranonymous@protonmail.com | ghostwriteranonymous@protonmail.com | drake_hill@owl-records.com | [EXTERNAL] Need a ghost... | CLEAN | http://betterlyrics4u.com/publish... |
| 2024-04-25 14:36:33.0000 | ghostwriteranonymous@protonmail.com | ghostwriteranonymous@protonmail.com | logic_white@owl-records.com | [EXTERNAL] Get FREE beat... | CLEAN | https://betterlyrics4u.com/free/mo... |

Less beef, more phish • Question 6 (solved): (30) points

Oh no! We've been phished!

Each of these rows represent an email that was sent to someone at OWL records!

Which email address was used to send most of these emails?

Hint: use the query from the previous question.

✓ ghostwritersanonymous@protonmail.com

Solved by 1995 players || Need help? Ask on discord @ [kc7cybercommunity](#)

Submit

kc7001.eastus

Run Recall KQL tools kc7001.eastus/OwlRecords

1 `let targets = Email`
2 `| where link has "betterjryics4u.com"`
3 `| distinct recipient;`
4 `Employees`
5 `| where email_addr in (_targets)`
6

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

/Path: /sender Inline Compact

1 "timestamp": 2024-04-10T14:45:28Z,
2 "sender": ghostwritersanonymous@protonmail.com,
3 "reply_to": ghostwritersanonymous@protonmail.com,
4 "recipient": ice_blake@owl-records.com,
5 "subject": [EXTERNAL] Get FREE beats from the best hip hop writers in the game!!!,
6 "verdict": CLEAN,
7 "link": https://betterjryics4u.com/search/published/public/signup

| 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://betterjryics4u.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://betterjryics4u.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://betterjryics4u.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://betterjryics4u.com/module... |
| 2024-04-12 13:37:39.0000 | ghostwritersanonymous@protonmail.com | ghostwritersanonymous@protonmail.com | il_lee@owl-records.com | [EXTERNAL] Need a ghost... | CLEAN | https://betterjryics4u.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://betterjryics4u.com/share/fil... |
| 2024-04-15 11:07:12.0000 | ghostwritersanonymous@protonmail.com | ghostwritersanonymous@protonmail.com | drake_audrey@owl-records.com | [EXTERNAL] RE: Need a gh... | CLEAN | http://betterjryics4u.com/share/fo... |
| 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://betterjryics4u.com/share/fo... |
| 2024-04-17 09:48:37.0000 | ghostwritersanonymous@protonmail.com | ghostwritersanonymous@protonmail.com | justin_cole@owl-records.com | [EXTERNAL] RE:RE: Need a ... | CLEAN | https://betterjryics4u.com/online/... |
| 2024-04-17 09:48:37.0000 | ghostwritersanonymous@protonmail.com | ghostwritersanonymous@protonmail.com | chance_west@owl-records.com | [EXTERNAL] Need a ghost... | CLEAN | https://betterjryics4u.com/pub/sha... |
| 2024-04-19 10:45:27.0000 | ghostwritersanonymous@protonmail.com | ghostwritersanonymous@protonmail.com | drake_hill@owl-records.com | [EXTERNAL] Need a ghost... | CLEAN | https://betterjryics4u.com/pub/sha... |
| 2024-04-19 10:45:27.0000 | ghostwritersanonymous@protonmail.com | ghostwritersanonymous@protonmail.com | drake_hill@owl-records.com | [EXTERNAL] Need a ghost... | CLEAN | https://betterjryics4u.com/pub/sha... |
| 2024-04-25 14:36:53.0000 | ghostwritersanonymous@protonmail.com | ghostwritersanonymous@protonmail.com | logic_white@owl-records.com | [EXTERNAL] Get FREE beat... | CLEAN | https://betterjryics4u.com/files/mo... |

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

✓ wemakebeatz@gmail.com

Solved by 1935 players || Need help? Ask on discord @ [kc7cybercommunity](#)

Submit

Less beef, more phish • Question 8 (solved): (30) points

It looks like the adversaries were targeting users with very particular roles.

```
let _targets = Email
| where link has "betterjryics4u.com"
| distinct recipient;
Employees
| where email_addr in (_targets)
```

Copy

Which role was targeted the most of all?

✓ Rapper

Solved by 1995 players || Need help? Ask on discord @ [kc7cybercommunity](#)

Submit

kc7001.eastus

Run Recall KQL tools kc7001.eastus/OwlRecords

1 `let _targets = Email`
2 `| where link has "betterjryics4u.com"`
3 `| distinct recipient;`
4 `Employees`
5 `| where email_addr in (_targets)`
6

Table 1 + Add visual Stats Search UTC Done (0.824 s) 10 records

/Path: /hire_date Inline Compact

1 "hire_date": 2021-07-24T00:00:00Z,
2 "name": Chance West,
3 "user_agent": Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.110 Safari/537.36,
4 "ip_addr": 10.10.0.18,
5 "email_addr": chance_west@owl-records.com,
6 "company_domain": owl-records.com,
7 "username": chwest,

| hire_date | name | user_agent | ip_addr | email_addr | company_domain | username | role | hostname |
|--------------------------|-------------|---|------------|-----------------------------|-----------------|------------|--------|---------------|
| 2021-05-31 00:00:00.0000 | Drake Hill | Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.110 Safari/537.36 | 10.10.0.14 | drake_hill@owl-records.com | owl-records.com | drhill | Rapper | JWR3-LAPTOP |
| 2021-07-24 00:00:00.0000 | Chance West | Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.110 Safari/537.36 | 10.10.0.18 | chance_west@owl-records.com | owl-records.com | chwest | Rapper | QDR-DESKTOP |
| 2021-10-16 00:00:00.0000 | Nikki Lane | Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.110 Safari/537.36 | 10.10.0.26 | nikki_lane@owl-records.com | owl-records.com | nilane | Rapper | UCVH-MACH... |
| 2022-01-03 00:00:00.0000 | Li Zee | Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.3; Trident/4.0) | 10.10.0.16 | il_lee@owl-records.com | owl-records.com | ilcee | Rapper | OIHK-LAPTOP |
| 2022-02-16 00:00:00.0000 | Snoop Th... | Mozilla/5.0 (Windows NT 10.0; WOW64; rv47.0) Gecko/20100101 Firefox/4... | 10.10.0.21 | snoop_thompson@owl-recor... | owl-records.com | snthompson | Rapper | QISAC-LAPTOP |
| 2022-05-29 00:00:00.0000 | Jay Knight | Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0) | 10.10.0.8 | jay_knight@owl-records.com | owl-records.com | jaknight | Rapper | HUVN-DESKT... |
| 2022-08-22 00:00:00.0000 | Drake Au... | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.110 Safari/537.36 | 10.10.0.5 | drake_audrey@owl-records... | owl-records.com | draudrey | Lead | BZ2-DESKTOP |
| 2023-01-24 00:00:00.0000 | Logic White | Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 5.1; Win64; x64; Trident/4.0) | 10.10.0.20 | logic_white@owl-records.com | owl-records.com | lwwhite | Rapper | CUVH-MACH... |
| 2023-07-23 00:00:00.0000 | Justin Cole | Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.110 Safari/537.36 | 10.10.0.29 | justin_cole@owl-records.com | owl-records.com | jucole | Rapper | SHUW-MACH... |
| 2023-09-25 00:00:00.0000 | Ice Blake | Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 5.1; Win64; x64; Trident/4.0) | 10.10.0.24 | ice_blake@owl-records.com | owl-records.com | icblake | Rapper | IMVU-LAPTOP |

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 1000 players || Need help? Ask on discord @ [k2zydehcommunity](#)

Submit

kc7001.eastus

Run Recall KQL tools kc7001.eastus/OwlRecords

```
1 let _targets = email
2 | where link has "betterlyrics4u.com"
3 | distinct recipient;
4 Employees
5 | where email_addr in (_targets)
6
```

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 |
|----------------------------|---------------|---|------------|--------------------------------|-----------------|----------|---------|--------------|
| > 2021-05-21 00:00:00.0000 | Drake Hill | Mozilla/5.0 (Windows NT 6.1; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.104 Safari/537.36 | 10.10.0.14 | drake_hill@owl-records.com | owl-records.com | dhill | Rapper | XWR2-LAPTOP |
| > 2021-07-24 00:00:00.0000 | Chance West | Mozilla/5.0 (Windows NT 6.1; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.104 Safari/537.36 | 10.10.0.18 | chance_west@owl-records.com | owl-records.com | chwest | Rapper | QJGR-DESKTOP |
| > 2021-10-18 00:00:00.0000 | Nikki Lane | Mozilla/5.0 (Windows NT 6.1; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.104 Safari/537.36 | 10.10.0.28 | nikki_lane@owl-records.com | owl-records.com | nlane | Rapper | UCVH-MACH... |
| > 2022-01-23 00:00:00.0000 | Li Zea | Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0) | 10.10.0.16 | li_zea@owl-records.com | owl-records.com | lzea | Rapper | OWH-LAPTOP |
| > 2022-03-16 00:00:00.0000 | Snoop Th. | Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/44.0 | 10.10.0.21 | snoop_thompson@owl-records.com | owl-records.com | stompson | Rapper | QJAC-LAPTOP |
| > 2022-05-29 00:00:00.0000 | Jay Knight | Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0) | 10.10.0.8 | jay_knight@owl-records.com | owl-records.com | jknight | Rapper | HUVH-DESK... |
| > 2022-05-22 00:00:00.0000 | Dwaine Audrey | Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.104 Safari/537.36 | 10.10.0.5 | dwaine_audrey@owl-records.com | owl-records.com | dwaudrey | Lead... | 8SD-DESKTOP |

1 Lead Rapper

Less beef, more phish • Question 12 (solved): (30) points

Let's take a look at those emails again!

Email
| where link has "betterlyrics4u.com"

What was the subject of the email sent to Dwake?

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

Solved by 1000 players || Need help? Ask on discord @ [k2zydehcommunity](#)

Submit

kc7001.eastus

Run Recall KQL tools kc7001.eastus/OwlRecords

```
1 Email
2 | 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 |
|----------------------------|---------------------------------------|---------------------------------------|-------------------------------|-----------------------------|---------|---|
| > 2024-04-10 14:45:28.0000 | ghostwrittersanonymous@protonmail.com | ghostwrittersanonymous@protonmail.com | ice_blaize@owl-records.com | [EXTERNAL] Get FREE beat... | CLEAN | https://betterlyrics4u.com/search/... |
| > 2024-04-10 14:45:28.0000 | ghostwrittersanonymous@protonmail.com | ghostwrittersanonymous@protonmail.com | nikki_lane@owl-records.com | [EXTERNAL] Get FREE beat... | CLEAN | https://betterlyrics4u.com/search/... |
| > 2024-04-11 08:50:10.0000 | wemakebeats@gmail.com | wemakebeats@gmail.com | jay_knight@owl-records.com | [EXTERNAL] FW: Get FREE ... | BLOCKED | https://betterlyrics4u.com/module/... |
| > 2024-04-11 08:50:10.0000 | wemakebeats@gmail.com | wemakebeats@gmail.com | jay_knight@owl-records.com | [EXTERNAL] FW: Get FREE ... | BLOCKED | https://betterlyrics4u.com/module/... |
| > 2024-04-12 13:37:39.0000 | ghostwrittersanonymous@protonmail.com | ghostwrittersanonymous@protonmail.com | li_zea@owl-records.com | [EXTERNAL] Need a ghost... | CLEAN | https://betterlyrics4u.com/share/fil... |
| > 2024-04-12 13:37:39.0000 | ghostwrittersanonymous@protonmail.com | ghostwrittersanonymous@protonmail.com | jay_knight@owl-records.com | [EXTERNAL] Need a ghost... | CLEAN | https://betterlyrics4u.com/share/fil... |
| > 2024-04-15 11:07:12.0000 | ghostwrittersanonymous@protonmail.com | ghostwrittersanonymous@protonmail.com | dwaine_audrey@owl-records.com | [EXTERNAL] RE: Need a gh... | CLEAN | http://betterlyrics4u.com/share/onl... |

JPath /subject Inline Compact

```
2 "sender": ghostwrittersanonymous@protonmail.com,
3 "reply_to": ghostwrittersanonymous@protonmail.com,
4 "recipient": dwaine_audrey@owl-records.com,
5 "subject": [EXTERNAL] RE: Need a ghostwriter for your next hit?,
6 "verdict": CLEAN,
7 "link": http://betterlyrics4u.com/share/online/published/enter
8
```

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 1000 players || Need help? Ask on discord @ [k2zydehcommunity](#)

Submit

kc7001.eastus

Run Recall KQL tools kc7001.eastus/OwlRecords

```
1 Email
2 | 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 |
|----------------------------|---------------------------------------|---------------------------------------|-------------------------------|-----------------------------|---------|---|
| > 2024-04-10 14:45:28.0000 | ghostwrittersanonymous@protonmail.com | ghostwrittersanonymous@protonmail.com | ice_blaize@owl-records.com | [EXTERNAL] Get FREE beat... | CLEAN | https://betterlyrics4u.com/search/... |
| > 2024-04-10 14:45:28.0000 | ghostwrittersanonymous@protonmail.com | ghostwrittersanonymous@protonmail.com | nikki_lane@owl-records.com | [EXTERNAL] Get FREE beat... | CLEAN | https://betterlyrics4u.com/search/... |
| > 2024-04-11 08:50:10.0000 | wemakebeats@gmail.com | wemakebeats@gmail.com | jay_knight@owl-records.com | [EXTERNAL] FW: Get FREE ... | BLOCKED | https://betterlyrics4u.com/module/... |
| > 2024-04-11 08:50:10.0000 | wemakebeats@gmail.com | wemakebeats@gmail.com | jay_knight@owl-records.com | [EXTERNAL] FW: Get FREE ... | BLOCKED | https://betterlyrics4u.com/module/... |
| > 2024-04-12 13:37:39.0000 | ghostwrittersanonymous@protonmail.com | ghostwrittersanonymous@protonmail.com | li_zea@owl-records.com | [EXTERNAL] Need a ghost... | CLEAN | https://betterlyrics4u.com/share/fil... |
| > 2024-04-12 13:37:39.0000 | ghostwrittersanonymous@protonmail.com | ghostwrittersanonymous@protonmail.com | jay_knight@owl-records.com | [EXTERNAL] Need a ghost... | CLEAN | https://betterlyrics4u.com/share/fil... |
| > 2024-04-15 11:07:12.0000 | ghostwrittersanonymous@protonmail.com | ghostwrittersanonymous@protonmail.com | dwaine_audrey@owl-records.com | [EXTERNAL] RE: Need a gh... | CLEAN | http://betterlyrics4u.com/share/onl... |

JPath /link Inline Compact

```
2 "sender": ghostwrittersanonymous@protonmail.com,
3 "reply_to": ghostwrittersanonymous@protonmail.com,
4 "recipient": dwaine_audrey@owl-records.com,
5 "subject": [EXTERNAL] RE: Need a ghostwriter for your next hit?,
6 "verdict": CLEAN,
7 "link": http://betterlyrics4u.com/share/online/published/enter
8
```

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 1000 players | Need help? Ask on discord @ [kz2vibe/community](#)

Submit

kc7001.eastus

kc7001.eastus.OwlR...

Run

Recall

KQL tools

kc7001.eastus/OwlRecords

Pin to dashboard

Open

Copy

Export

1 Email

2 | 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 |
|----------------------------|-------------------------------------|-------------------------------------|------------------------------|-----------------------------|---------|---|
| > 2024-04-10 14:45:28.0000 | ghostwritersanonymou@protonmail.com | ghostwritersanonymou@protonmail.com | ke_hale@owl-records.com | [EXTERNAL] Get FREE beat... | CLEAN | https://betterlyrics4u.com/search/... |
| > 2024-04-10 14:45:28.0000 | ghostwritersanonymou@protonmail.com | ghostwritersanonymou@protonmail.com | nikki_lane@owl-records.com | [EXTERNAL] Get FREE beat... | CLEAN | https://betterlyrics4u.com/search/... |
| > 2024-04-11 08:50:10.0000 | wemakebeats@gmail.com | ghostwritersanonymou@protonmail.com | jay_knight@owl-records.com | [EXTERNAL] FW: Get FREE... | BLOCKED | https://betterlyrics4u.com/module... |
| > 2024-04-11 08:50:10.0000 | wemakebeats@gmail.com | wemakebeats@gmail.com | jay_knight@owl-records.com | [EXTERNAL] FW: Get FREE... | BLOCKED | https://betterlyrics4u.com/module... |
| > 2024-04-12 13:37:39.0000 | ghostwritersanonymou@protonmail.com | ghostwritersanonymou@protonmail.com | li_zee@owl-records.com | [EXTERNAL] Need a ghost... | CLEAN | https://betterlyrics4u.com/share/fli... |
| > 2024-04-12 13:37:39.0000 | ghostwritersanonymou@protonmail.com | ghostwritersanonymou@protonmail.com | jay_knight@owl-records.com | [EXTERNAL] Need a ghost... | CLEAN | https://betterlyrics4u.com/share/fli... |
| > 2024-04-15 11:07:12.0000 | ghostwritersanonymou@protonmail.com | ghostwritersanonymou@protonmail.com | dwake_audrey@owl-records.com | [EXTERNAL] RE: Need a gh... | CLEAN | http://betterlyrics4u.com/share/on... |

JPath

/link

Inline

Compact

2 "sender": ghostwritersanonymou@protonmail.com,

3 "reply_to": ghostwritersanonymou@protonmail.com,

4 "recipient": dwake_audrey@owl-records.com,

5 "subject": [EXTERNAL] RE: Need a ghostwriter for your next hit,

6 "verdict": CLEAN,

7 "link": http://betterlyrics4u.com/share/online/published/enter

8

> 2024-04-15 11:07:12.0000

ghostwritersanonymou@protonmail.com

ghostwritersanonymou@protonmail.com

snoop.thompson@owl-records.com

[EXTERNAL] RE: Need a gh...

CLEAN

<http://betterlyrics4u.com/share/on...>

> 2024-04-17 09:48:27.0000

ghostwritersanonymou@protonmail.com

ghostwritersanonymou@protonmail.com

justin_cole@owl-records.com

[EXTERNAL] RE: RE: Need a ...

CLEAN

<https://betterlyrics4u.com/online/...>

> 2024-04-17 09:48:27.0000

ghostwritersanonymou@protonmail.com

ghostwritersanonymou@protonmail.com

charice_west@owl-records.com

[EXTERNAL] RE: RE: Need a ...

CLEAN

<https://betterlyrics4u.com/online/...>

> 2024-04-19 13:45:27.0000

ghostwritersanonymou@protonmail.com

ghostwritersanonymou@protonmail.com

drake_hill@owl-records.com

[EXTERNAL] Need a ghost...

CLEAN

<http://betterlyrics4u.com/publish...>

> 2024-04-19 13:45:27.0000

ghostwritersanonymou@protonmail.com

ghostwritersanonymou@protonmail.com

drake_hill@owl-records.com

[EXTERNAL] Need a ghost...

CLEAN

<http://betterlyrics4u.com/publish...>

> 2024-04-25 14:36:33.0000

ghostwritersanonymou@protonmail.com

ghostwritersanonymou@protonmail.com

logic_white@owl-records.com

[EXTERNAL] Get FREE beat...

CLEAN

<https://betterlyrics4u.com/files/mo...>

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?

Block

Ghost Writer

to me

9:35 PM (5 hours ago)

☆ ↻ ⋮

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 adversaries sign the email with?

ghostwriter

Solved by 1000 players | Need help? Ask on discord @ [kz2vibe/community](#)

Submit

kc7001.eastus

kc7001.eastus.OwlR...

Run

Recall

KQL tools

kc7001.eastus/OwlRecords

Pin to dashboard

Open

Copy

Export

1 Email

2 | 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 |
|----------------------------|-------------------------------------|-------------------------------------|------------------------------|-----------------------------|---------|---|
| > 2024-04-10 14:45:28.0000 | ghostwritersanonymou@protonmail.com | ghostwritersanonymou@protonmail.com | ke_hale@owl-records.com | [EXTERNAL] Get FREE beat... | CLEAN | https://betterlyrics4u.com/search/... |
| > 2024-04-10 14:45:28.0000 | ghostwritersanonymou@protonmail.com | ghostwritersanonymou@protonmail.com | nikki_lane@owl-records.com | [EXTERNAL] Get FREE beat... | CLEAN | https://betterlyrics4u.com/search/... |
| > 2024-04-11 08:50:10.0000 | wemakebeats@gmail.com | ghostwritersanonymou@protonmail.com | jay_knight@owl-records.com | [EXTERNAL] FW: Get FREE... | BLOCKED | https://betterlyrics4u.com/module... |
| > 2024-04-11 08:50:10.0000 | wemakebeats@gmail.com | wemakebeats@gmail.com | jay_knight@owl-records.com | [EXTERNAL] FW: Get FREE... | BLOCKED | https://betterlyrics4u.com/module... |
| > 2024-04-12 13:37:39.0000 | ghostwritersanonymou@protonmail.com | ghostwritersanonymou@protonmail.com | li_zee@owl-records.com | [EXTERNAL] Need a ghost... | CLEAN | https://betterlyrics4u.com/share/fli... |
| > 2024-04-12 13:37:39.0000 | ghostwritersanonymou@protonmail.com | ghostwritersanonymou@protonmail.com | jay_knight@owl-records.com | [EXTERNAL] Need a ghost... | CLEAN | https://betterlyrics4u.com/share/fli... |
| > 2024-04-15 11:07:12.0000 | ghostwritersanonymou@protonmail.com | ghostwritersanonymou@protonmail.com | dwake_audrey@owl-records.com | [EXTERNAL] RE: Need a gh... | CLEAN | http://betterlyrics4u.com/share/on... |

JPath

/link

Inline

Compact

2 "sender": ghostwritersanonymou@protonmail.com,

3 "reply_to": ghostwritersanonymou@protonmail.com,

4 "recipient": dwake_audrey@owl-records.com,

5 "subject": [EXTERNAL] RE: Need a ghostwriter for your next hit,

6 "verdict": CLEAN,

7 "link": http://betterlyrics4u.com/share/online/published/enter

8

> 2024-04-15 11:07:12.0000

ghostwritersanonymou@protonmail.com

ghostwritersanonymou@protonmail.com

snoop.thompson@owl-records.com

[EXTERNAL] RE: Need a gh...

CLEAN

<http://betterlyrics4u.com/share/on...>

> 2024-04-17 09:48:27.0000

ghostwritersanonymou@protonmail.com

ghostwritersanonymou@protonmail.com

justin_cole@owl-records.com

[EXTERNAL] RE: RE: Need a ...

CLEAN

<https://betterlyrics4u.com/online/...>

> 2024-04-17 09:48:27.0000

ghostwritersanonymou@protonmail.com

ghostwritersanonymou@protonmail.com

charice_west@owl-records.com

[EXTERNAL] RE: RE: Need a ...

CLEAN

<https://betterlyrics4u.com/online/...>

> 2024-04-19 13:45:27.0000

ghostwritersanonymou@protonmail.com

ghostwritersanonymou@protonmail.com

drake_hill@owl-records.com

[EXTERNAL] Need a ghost...

CLEAN

<http://betterlyrics4u.com/publish...>

> 2024-04-19 13:45:27.0000

ghostwritersanonymou@protonmail.com

ghostwritersanonymou@protonmail.com

drake_hill@owl-records.com

[EXTERNAL] Need a ghost...

CLEAN

<http://betterlyrics4u.com/publish...>

> 2024-04-25 14:36:33.0000

ghostwritersanonymou@protonmail.com

ghostwritersanonymou@protonmail.com

logic_white@owl-records.com

[EXTERNAL] Get FREE beat...

CLEAN

<https://betterlyrics4u.com/files/mo...>