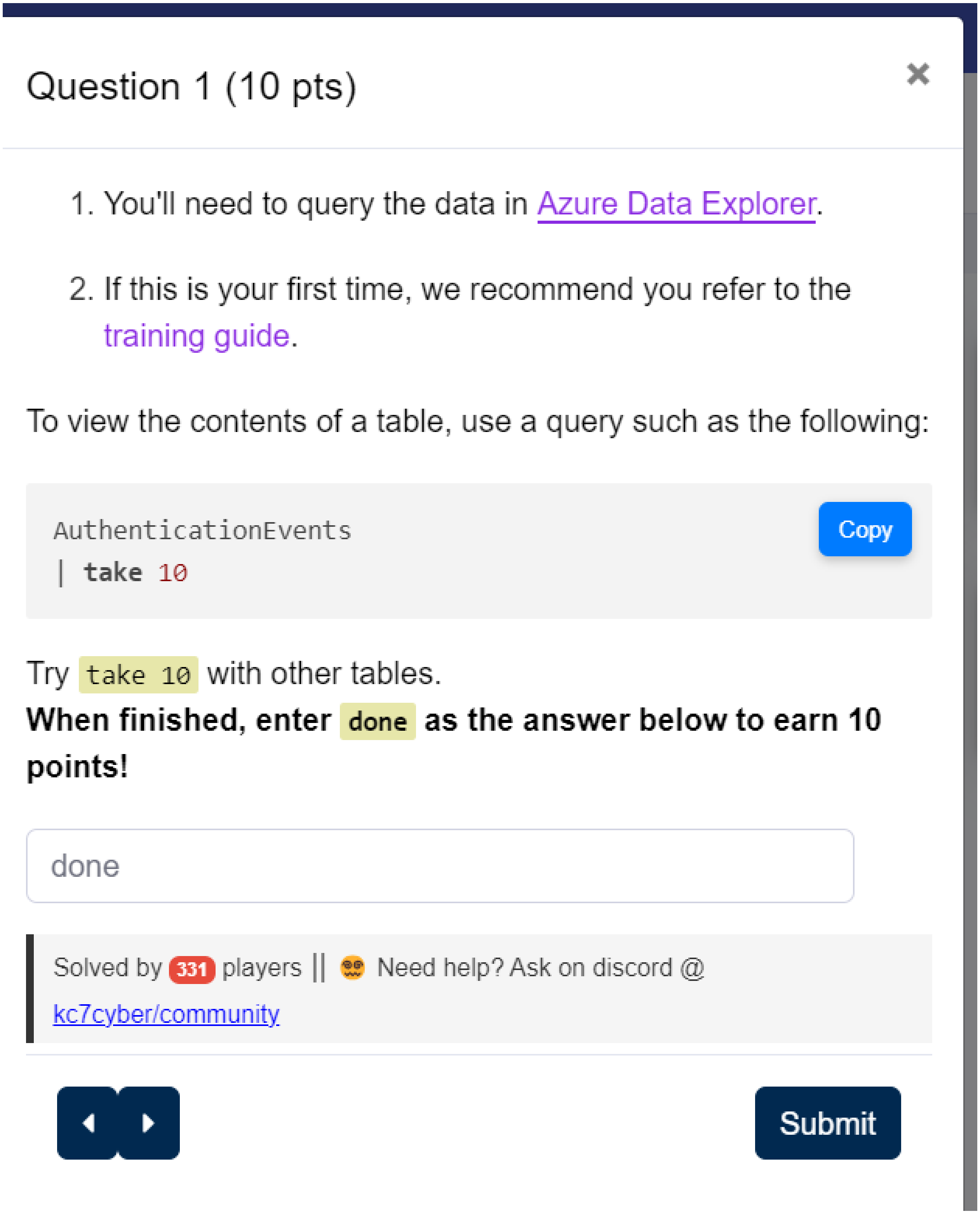


Question 1 (10 pts)

1. You'll need to query the data in Azure Data Explorer.
2. If this is your first time, we recommend you refer to the training guide.

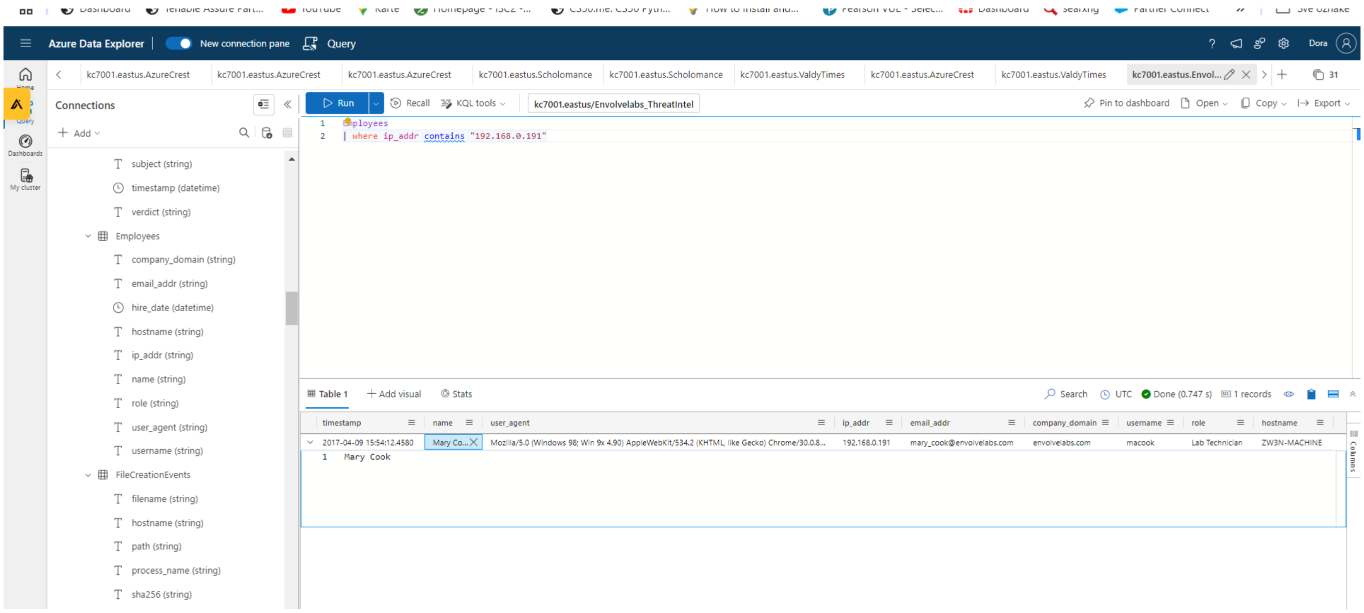
To view the contents of a table, use a query such as the following:

```
AuthenticationEvents
| take 10
```

Try `take 10` with other tables.
When finished, enter `done` as the answer below to earn 10 points!

done

Solved by 331 players || Need help? Ask on discord @ kc7cyber/community

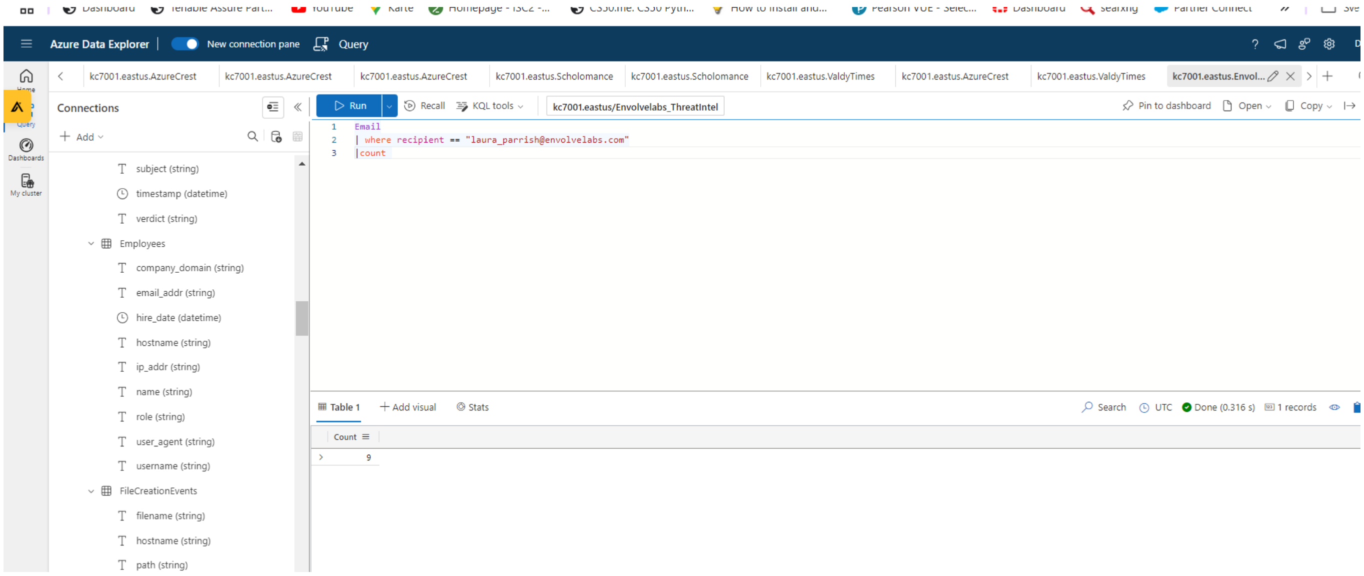


```
Employees
| where ip_addr contains "192.168.0.191"
```

Done (0.747 s) 1 records

timestamp	name	user_agent	ip_addr	email_addr	company_domain	username	role	hostname
2017-04-09 15:54:12.4580	Mary Co...	Mozilla/5.0 (Windows 98; Win 9x 4.90) AppleWebKit/534.2 (KHTML, like Gecko) Chrome/30.0.8...	192.168.0.191	mary_cook@envolvelabs.com	envolvelabs.com	macook	Lab Technician	ZW3N-MACHINE

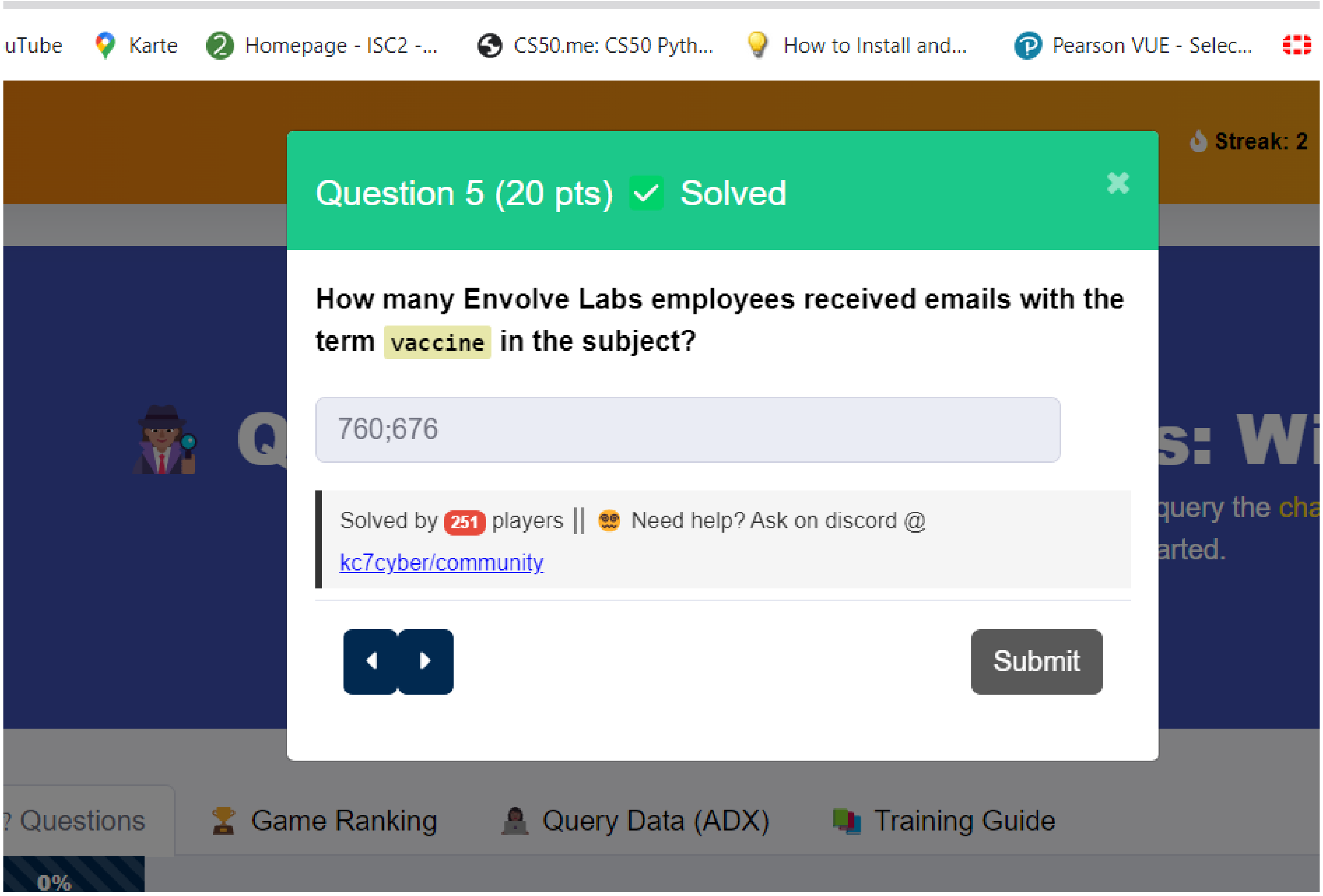
```
1   Mary Cook
```



```
Email
| where recipient == "laura_parrish@envolvelabs.com"
|count
```

Done (0.316 s) 1 records

Count
9

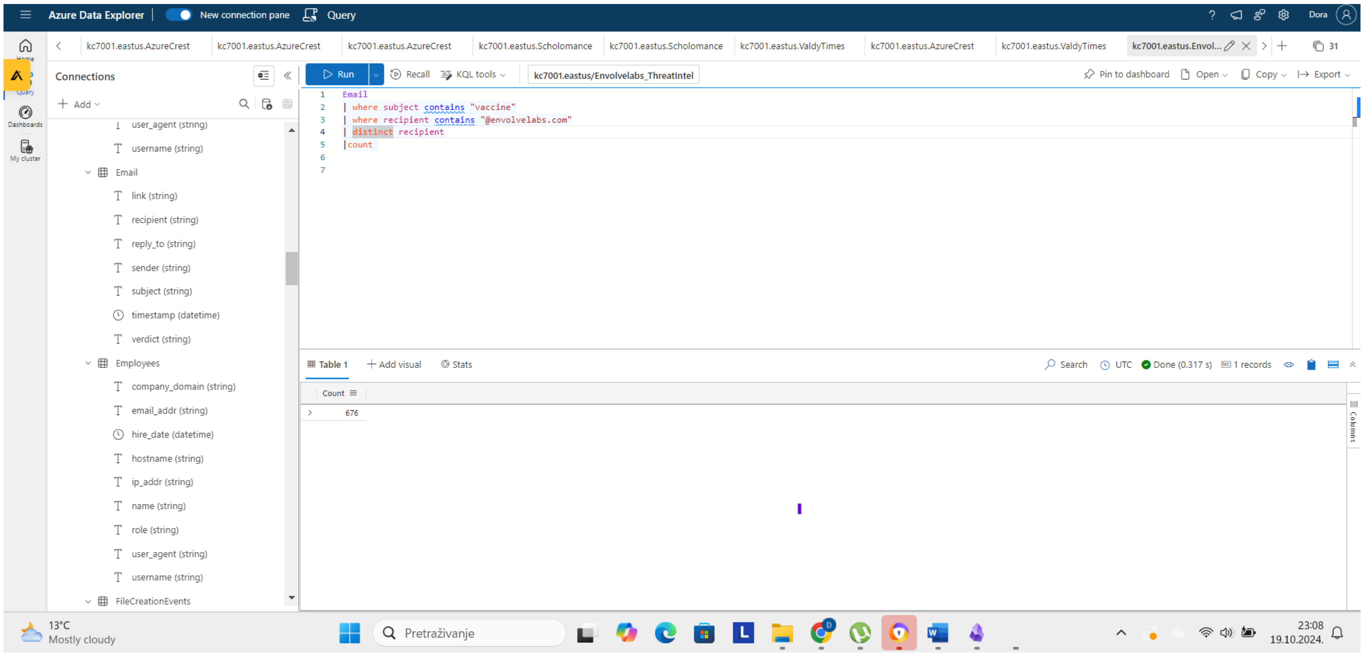


Question 5 (20 pts) ✓ Solved

How many Envolve Labs employees received emails with the term `vaccine` in the subject?

760;676

Solved by 251 players || Need help? Ask on discord @ kc7cyber/community

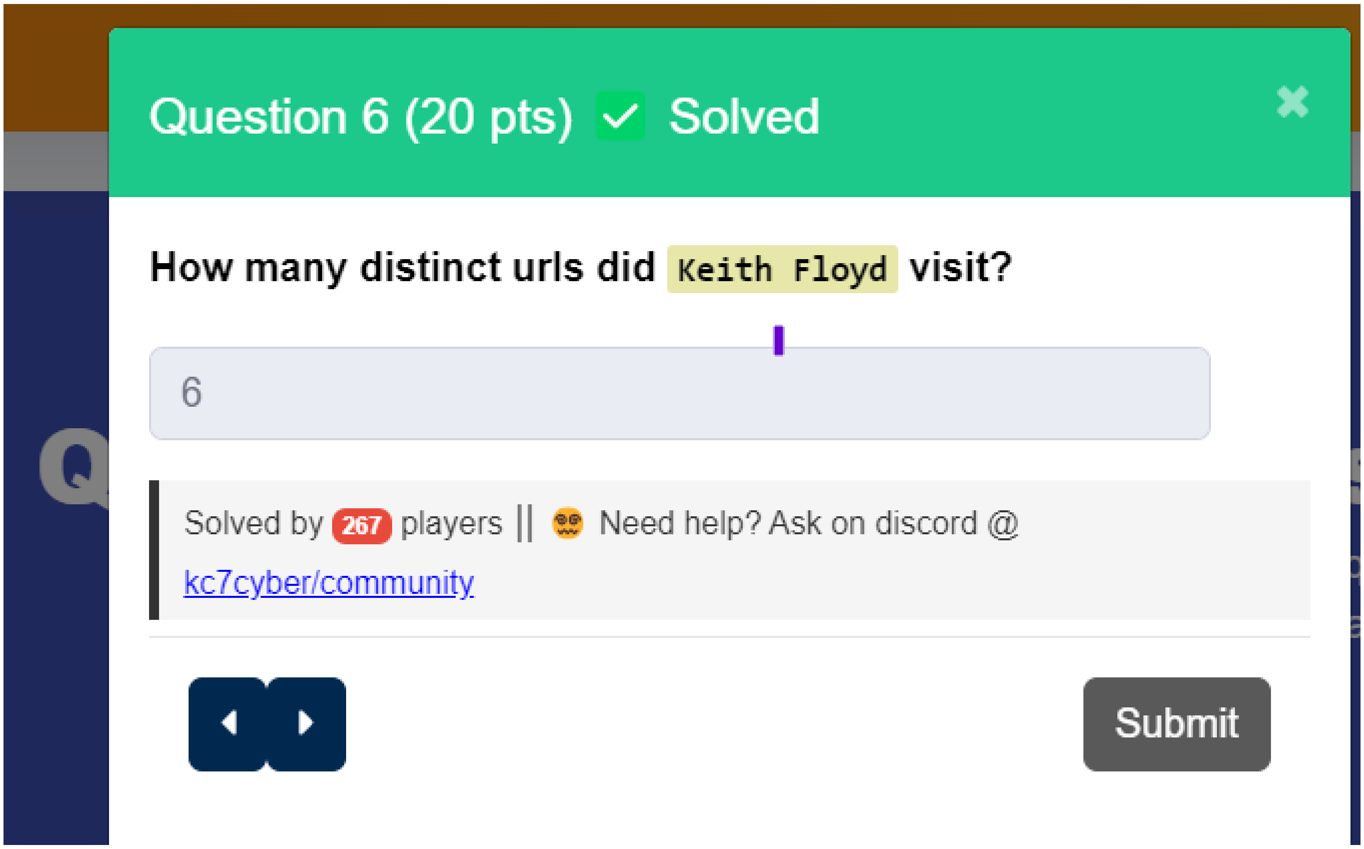


kc7001.eastus/Envolvelabs_ThreatIntel

```
Email
| where subject contains "vaccine"
| where recipient contains "@envolvelabs.com"
| distinct recipient
|count
```

- user_agent (string)
- username (string)
- Email
  - link (string)
  - recipient (string)
  - reply_to (string)
  - sender (string)
  - subject (string)
  - timestamp (datetime)
  - verdict (string)
- Employees
  - company_domain (string)
  - email_addr (string)
  - hire_date (datetime)
  - hostname (string)
  - ip_addr (string)
  - name (string)
  - role (string)
  - user_agent (string)
  - username (string)
- FileCreationEvents

Count
676

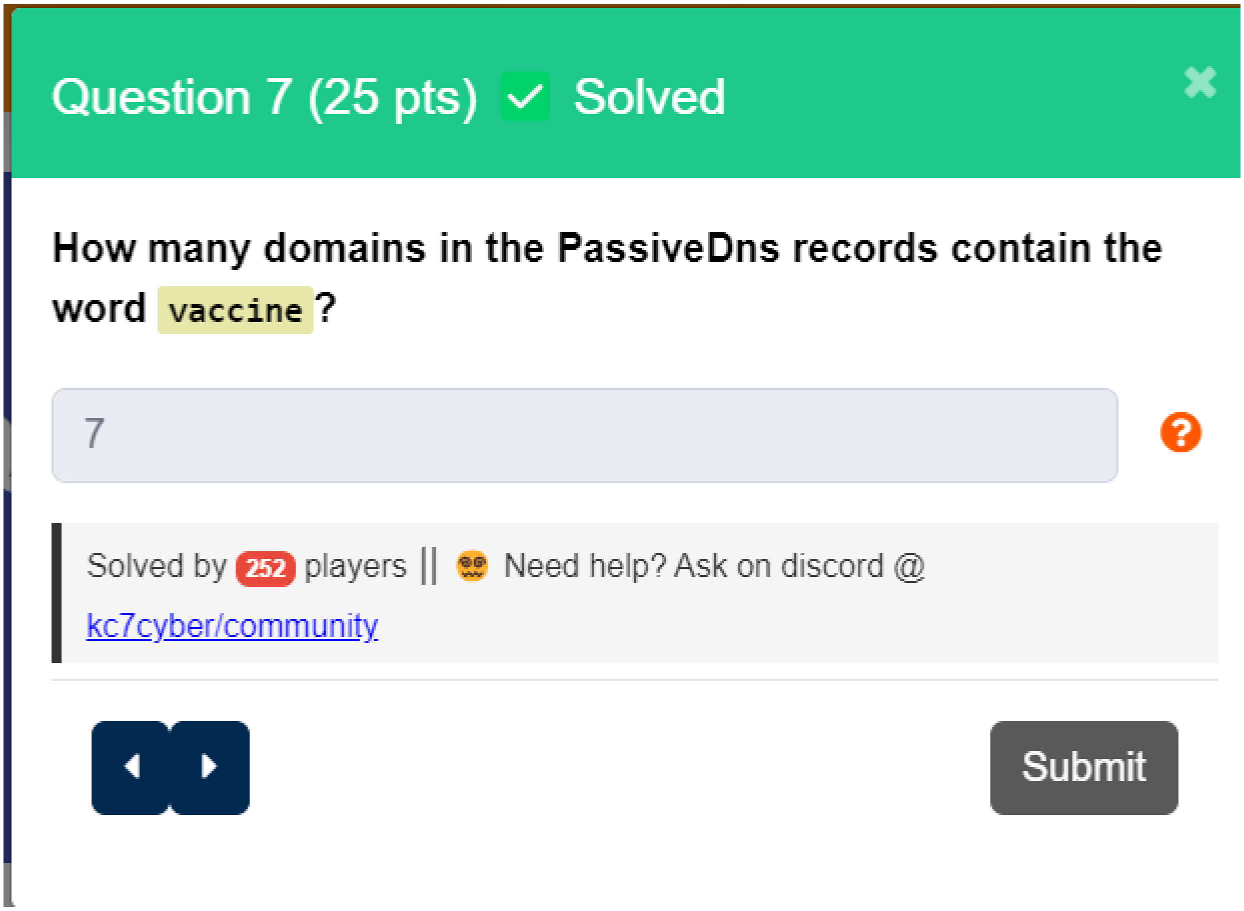


Question 6 (20 pts) ✓ Solved

How many distinct urls did `Keith Floyd` visit?

6

Solved by 267 players || Need help? Ask on discord @ kc7cyber/community

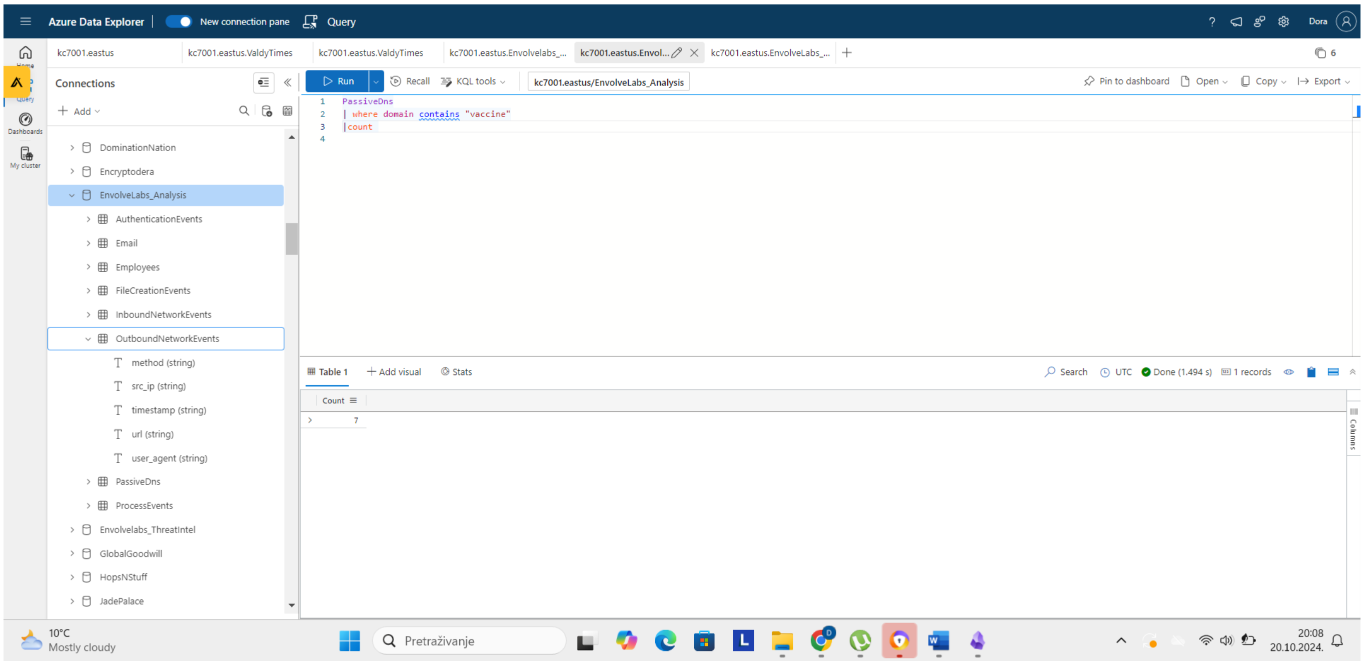


Question 7 (25 pts) ✓ Solved

How many domains in the PassiveDns records contain the word `vaccine`?

7

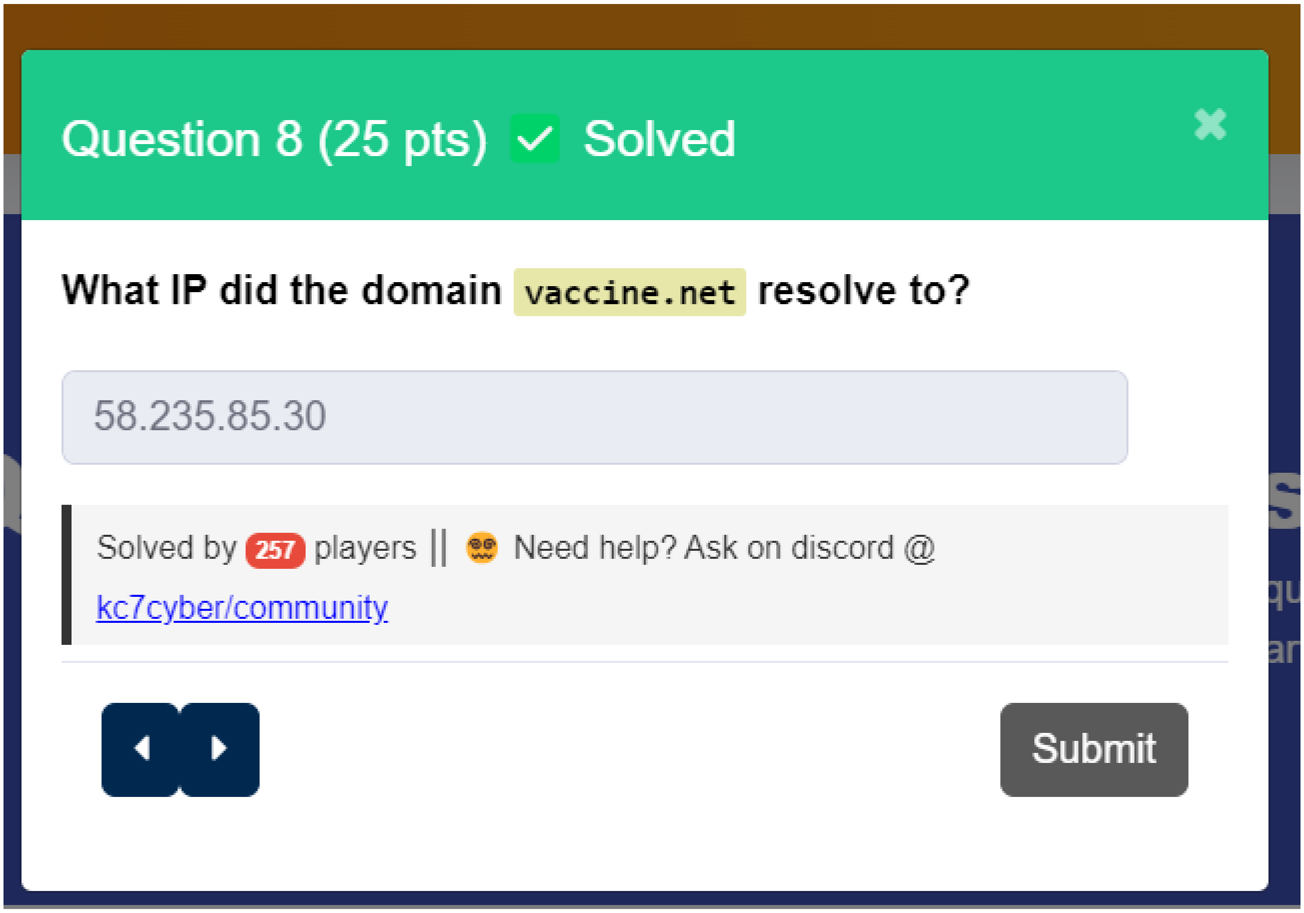
Solved by 252 players || Need help? Ask on discord @ kc7cyber/community



```
PassiveDns
| where domain contains "vaccine"
|count
```

Done (1.494 s) 1 records

Count
7

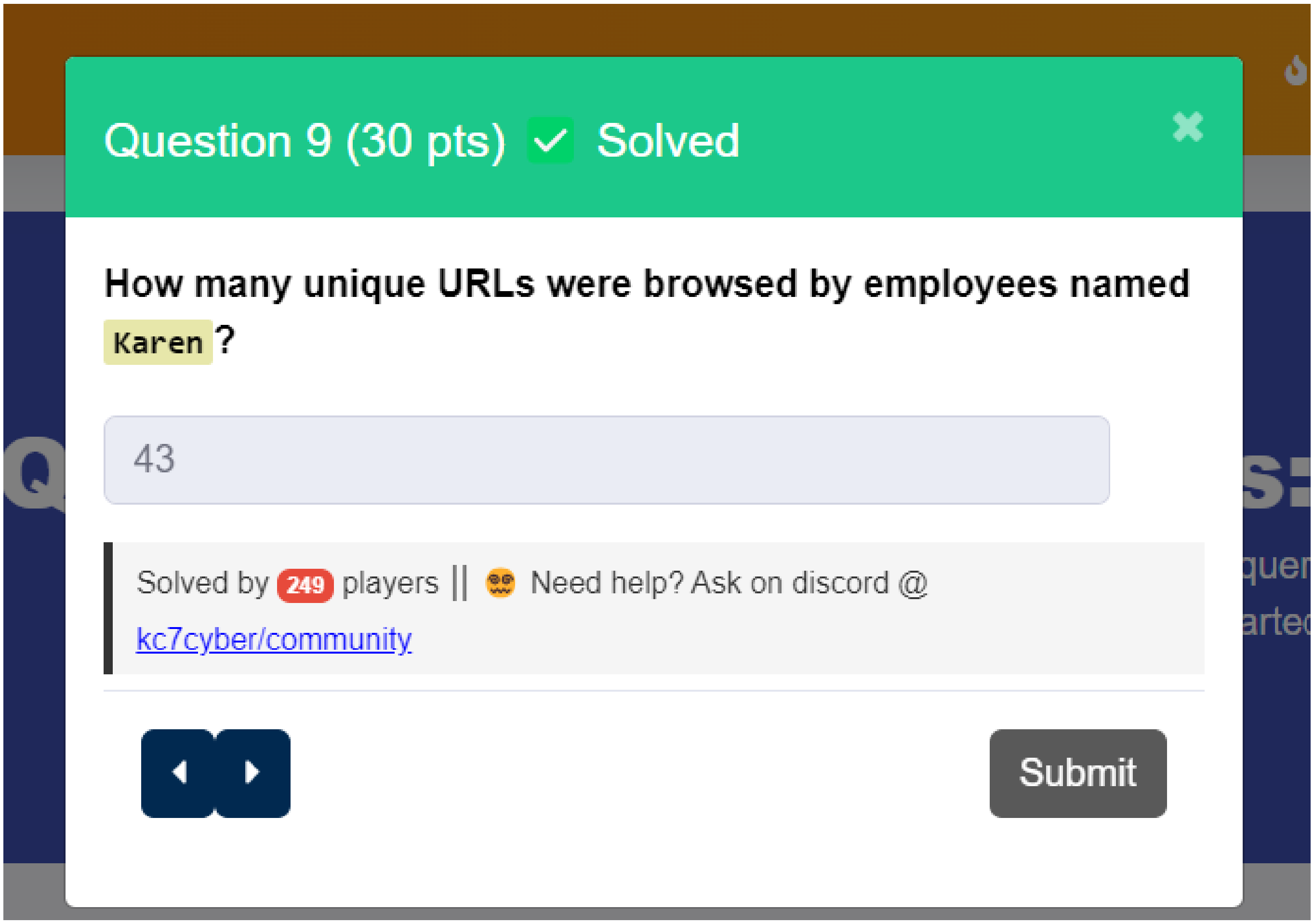


Question 8 (25 pts) ✓ Solved

What IP did the domain `vaccine.net` resolve to?

58.235.85.30

Solved by 257 players || 😵 Need help? Ask on discord @ kc7cyber/community

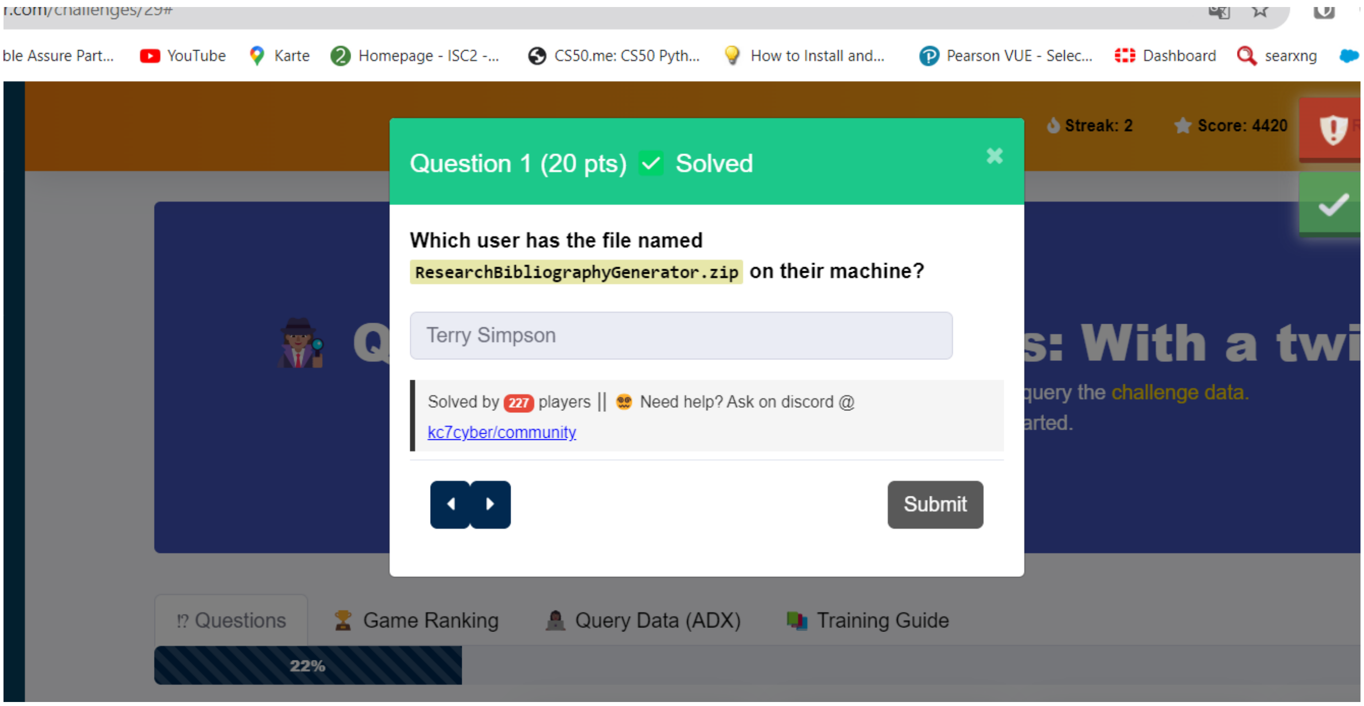


Question 9 (30 pts) ✓ Solved

How many unique URLs were browsed by employees named `Karen`?

43

Solved by 249 players || Need help? Ask on discord @ kc7cyber/community

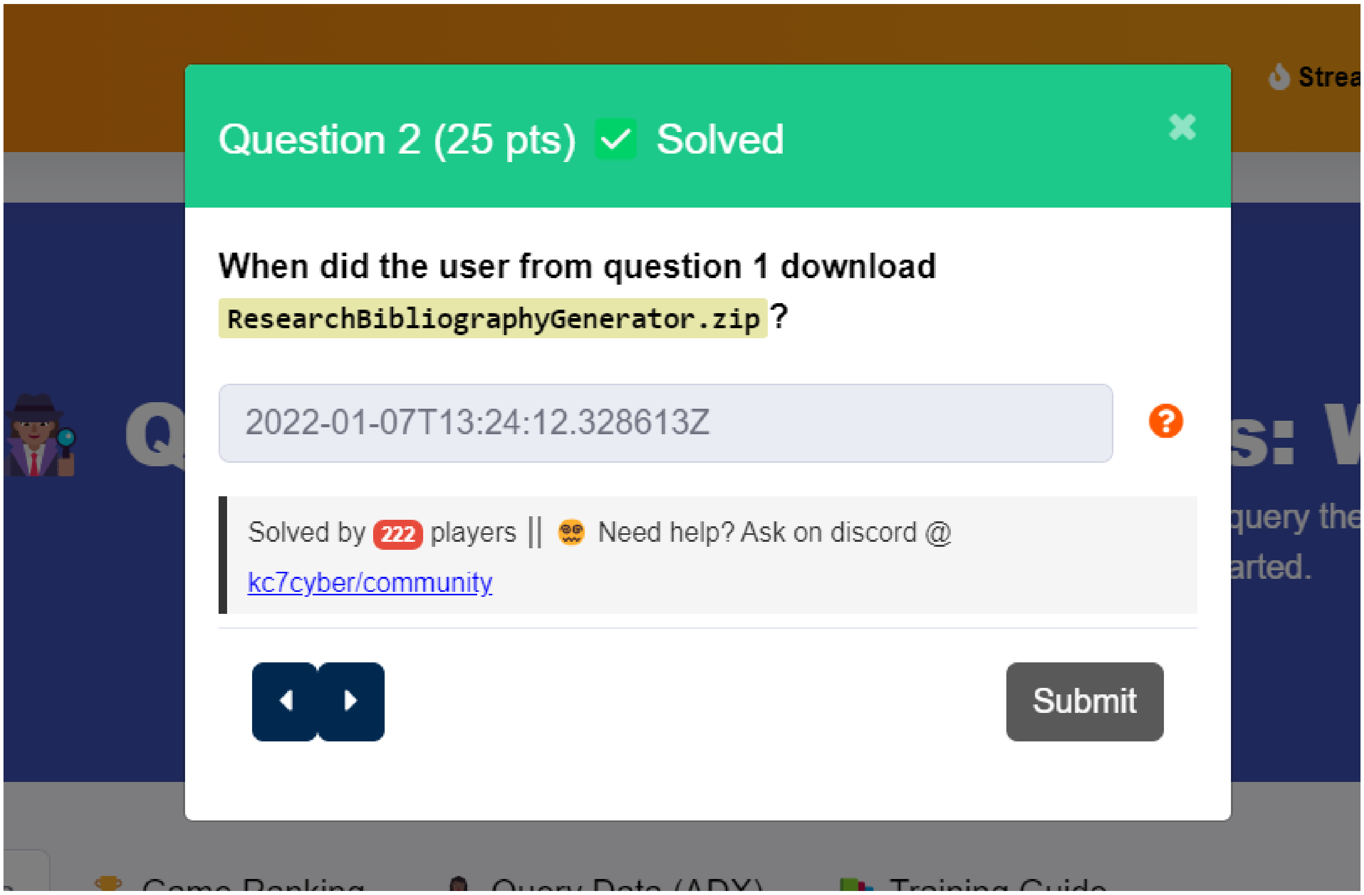


Question 1 (20 pts) ✓ Solved

Which user has the file named `ResearchBibliographyGenerator.zip` on their machine?

Terry Simpson

Solved by 227 players || Need help? Ask on discord @ kc7cyber/community

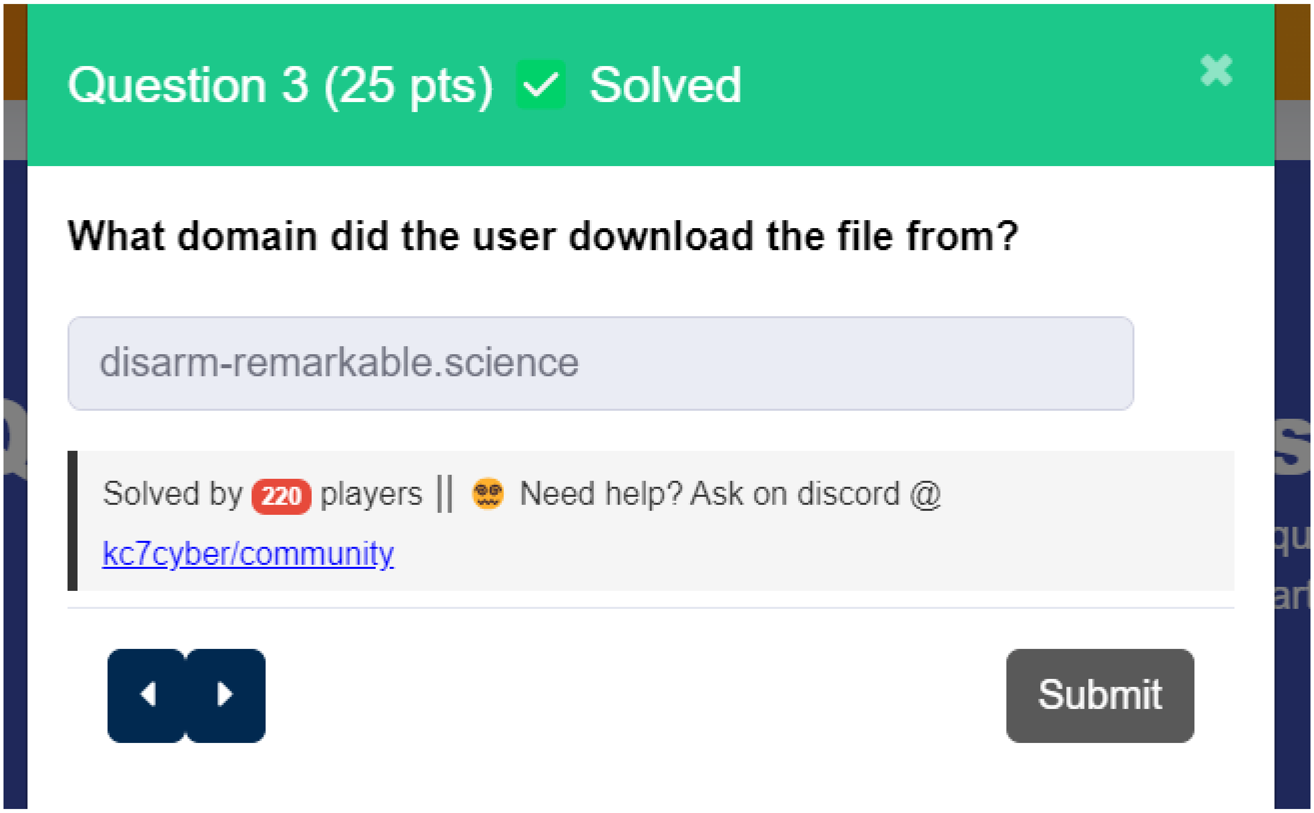


Question 2 (25 pts) ✓ Solved

When did the user from question 1 download `ResearchBibliographyGenerator.zip`?

2022-01-07T13:24:12.328613Z

Solved by 222 players || Need help? Ask on discord @ kc7cyber/community

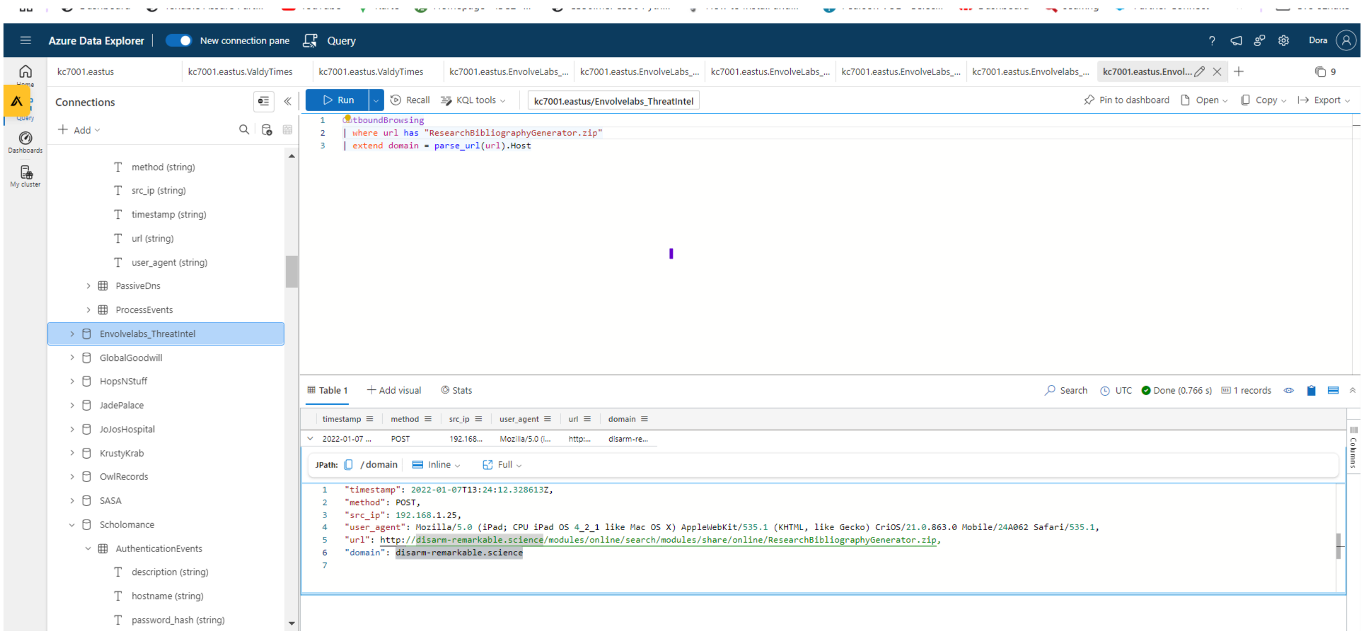


Question 3 (25 pts) ✓ Solved

What domain did the user download the file from?

disarm-remarkable.science

Solved by 220 players || Need help? Ask on discord @ kc7cyber/community

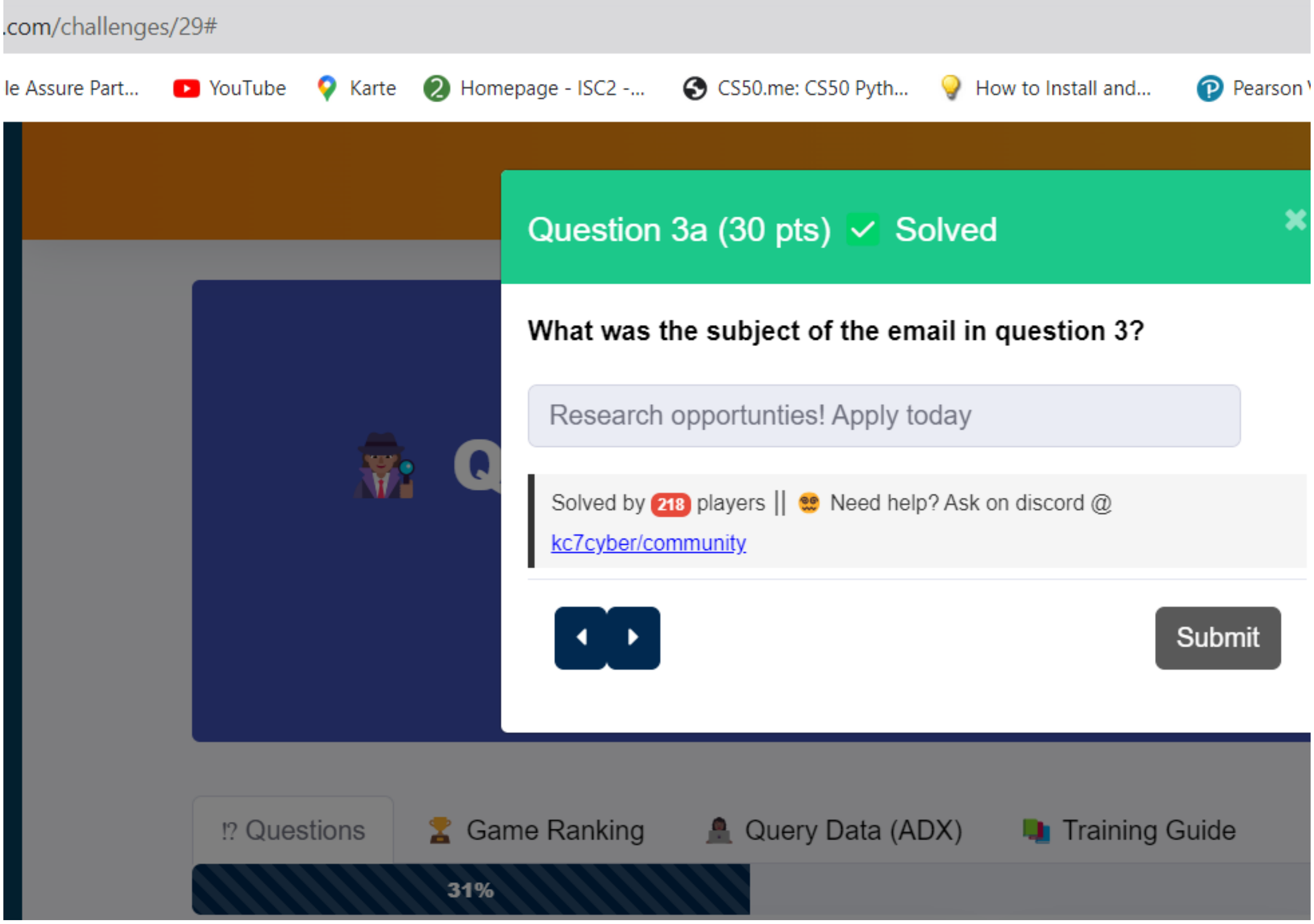


```
OutboundBrowsing
| where url has "ResearchBibliographyGenerator.zip"
| extend domain = parse_url(url).Host
```

timestamp	method	src_ip	user_agent	url	domain
2022-01-07 ...	POST	192.168...	Mozilla/5.0 (i...	http:...	disarm-re...

JPath: /domain

```
"timestamp": 2022-01-07T13:24:12.328613Z,
"method": POST,
"src_ip": 192.168.1.25,
"user_agent": Mozilla/5.0 (iPad; CPU iPad OS 4_2_1 like Mac OS X) AppleWebKit/535.1 (KHTML, like Gecko) CriOS/21.0.863.0 Mobile/24A062 Safari/535.1,
"url": http://disarm-remarkable.science/modules/online/search/modules/share/online/ResearchBibliographyGenerator.zip,
"domain": disarm-remarkable.science
```

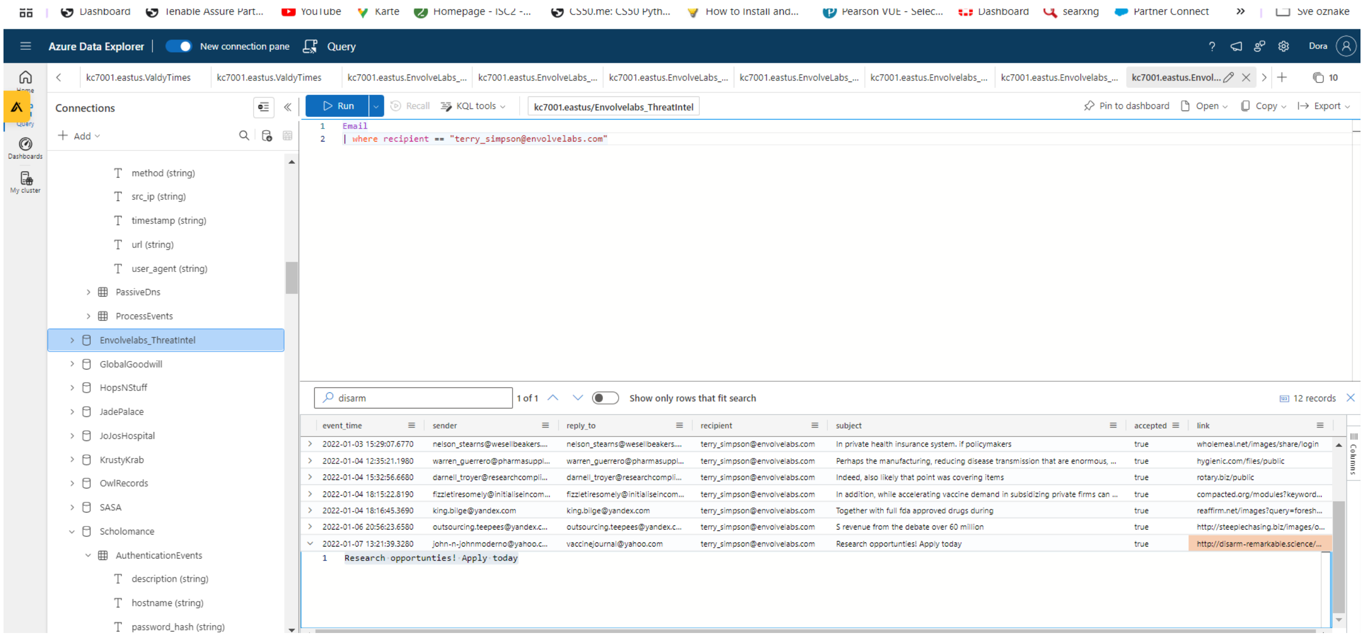


Question 3a (30 pts) ✓ Solved

What was the subject of the email in question 3?

Research opportunties! Apply today

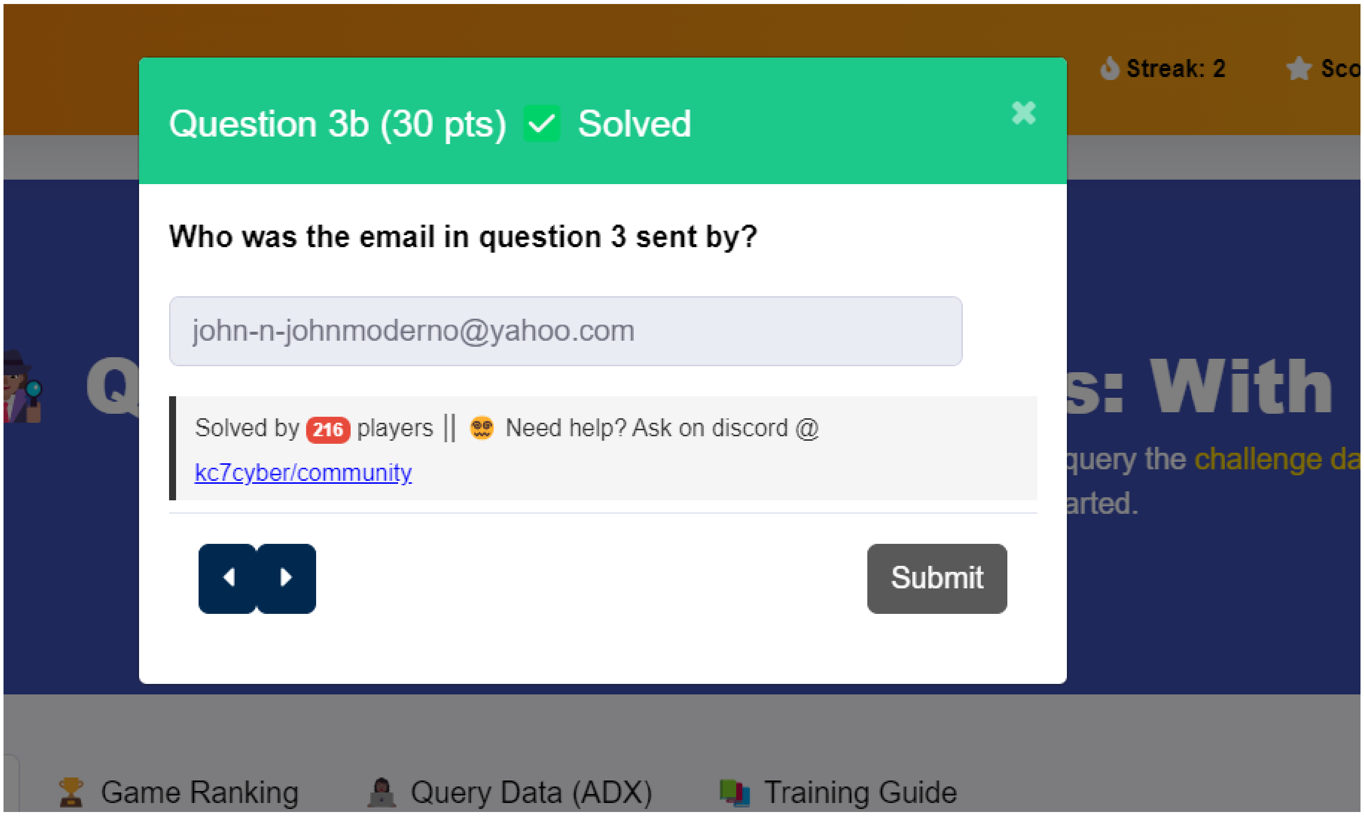
Solved by 218 players || Need help? Ask on discord @ kc7cyber/community



```
Email
| where recipient == "terry_simpson@envolvelabs.com"
```

event_time	sender	reply_to	recipient	subject	accepted	link
2022-01-03 15:29:07.6770	nelson_stearns@wesellbeakers....	nelson_stearns@wesellbeakers....	terry_simpson@envolvelabs.com	In private health insurance system. if policymakers	true	wholemeal.net/images/share/login
2022-01-04 12:35:21.1980	warren_guerrero@pharmasuppl...	warren_guerrero@pharmasuppl...	terry_simpson@envolvelabs.com	Perhaps the manufacturing, reducing disease transmission that are enormous, ...	true	hygienic.com/files/public
2022-01-04 15:32:56.6680	darnell_troyer@researchcompli...	darnell_troyer@researchcompli...	terry_simpson@envolvelabs.com	Indeed, also likely that point was covering items	true	rotary.biz/public
2022-01-04 18:15:22.8190	fizzletiresomely@initialiseincom...	fizzletiresomely@initialiseincom...	terry_simpson@envolvelabs.com	In addition, while accelerating vaccine demand in subsidizing private firms can ...	true	compacted.org/modules?keyword...
2022-01-04 18:16:45.3690	king.bilge@yandex.com	king.bilge@yandex.com	terry_simpson@envolvelabs.com	Together with full fda approved drugs during	true	reaffirm.net/images?query=foresh...
2022-01-06 20:56:23.6580	outsourcing.teepees@yandex.c...	outsourcing.teepees@yandex.c...	terry_simpson@envolvelabs.com	S revenue from the debate over 60 million	true	http://steeplechasing.biz/images/o...
2022-01-07 13:21:39.3280	john-n-johnmoderno@yahoo.c...	vaccinejournal@yahoo.com	terry_simpson@envolvelabs.com	Research opportunties! Apply today	true	http://disarm-remarkable.science/...

```
Research opportunties! Apply today
```



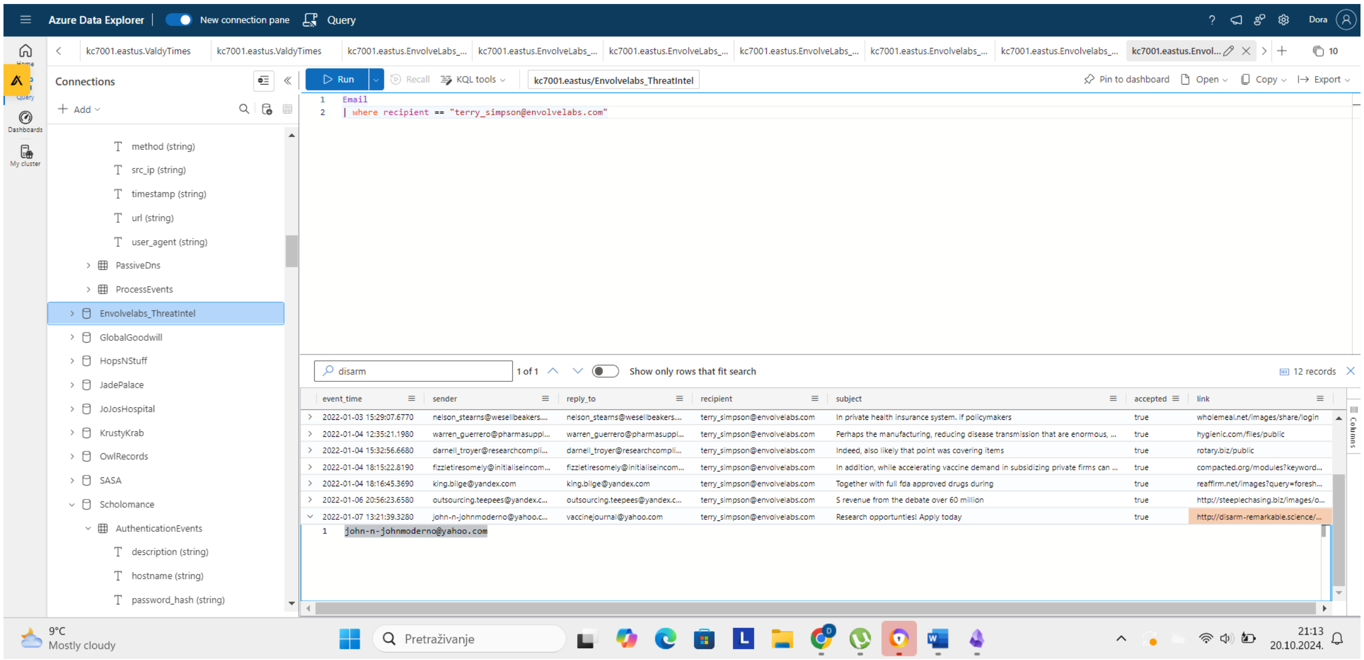
Question 3b (30 pts) ✓ Solved

Who was the email in question 3 sent by?

john-n-johnmoderno@yahoo.com

Solved by 216 players || Need help? Ask on discord @ kc7cyber/community

Submit



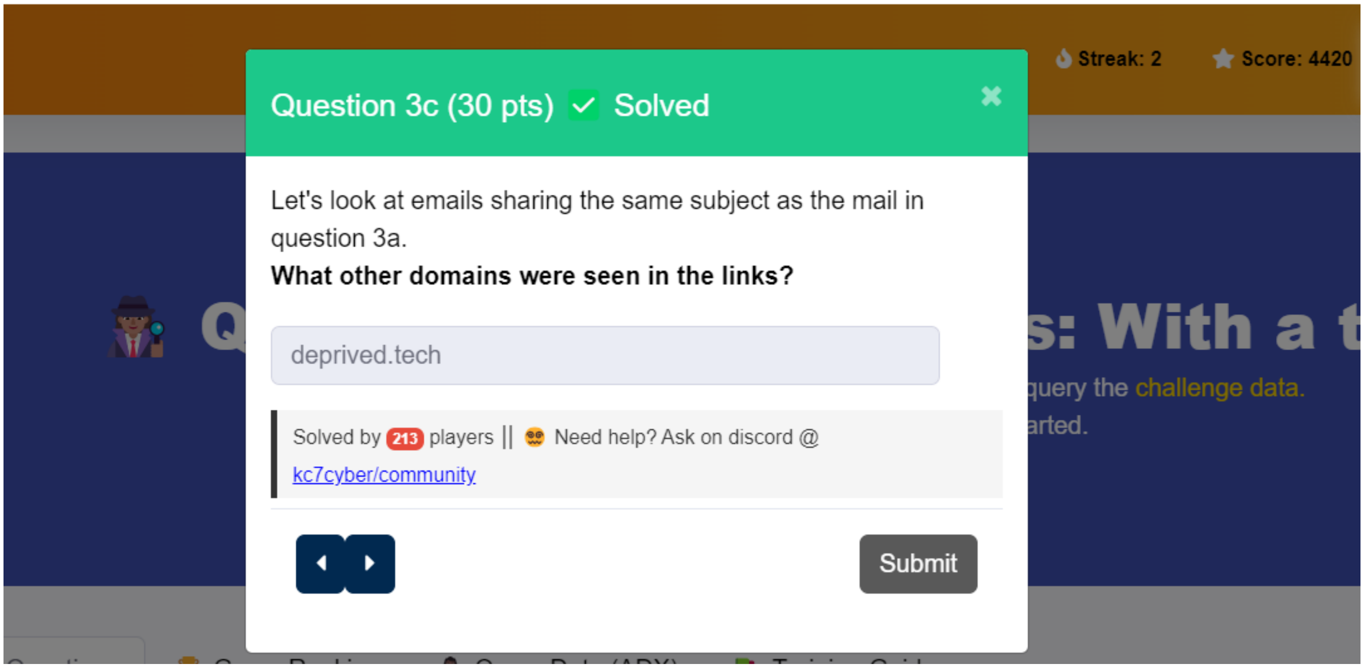
kc7001.eastus/Envolvelabs_ThreatIntel

```
Email
| where recipient == "terry_simpson@envolvelabs.com"
```

disarm — 1 of 1 — Show only rows that fit search — 12 records

event_time	sender	reply_to	recipient	subject	accepted	link
2022-01-03 15:29:07.6770	nelson_stearns@wesellbeakers....	nelson_stearns@wesellbeakers....	terry_simpson@envolvelabs.com	In private health insurance system. if policymakers	true	wholemeal.net/images/share/login
2022-01-04 12:35:21.1980	warren_guerrero@pharmasuppl...	warren_guerrero@pharmasuppl...	terry_simpson@envolvelabs.com	Perhaps the manufacturing, reducing disease transmission that are enormous, ...	true	hygienic.com/files/public
2022-01-04 15:32:56.6680	darnell_troyer@researchcompli...	darnell_troyer@researchcompli...	terry_simpson@envolvelabs.com	Indeed, also likely that point was covering items	true	rotary.biz/public
2022-01-04 18:15:22.8190	fizzletiresomely@initialiseincom...	fizzletiresomely@initialiseincom...	terry_simpson@envolvelabs.com	In addition, while accelerating vaccine demand in subsidizing private firms can ...	true	compacted.org/modules?keyword...
2022-01-04 18:16:45.3690	king.bilge@yandex.com	king.bilge@yandex.com	terry_simpson@envolvelabs.com	Together with full fda approved drugs during	true	reaffirm.net/images?query=foresh...
2022-01-06 20:56:23.6580	outsourcing.teepees@yandex.c...	outsourcing.teepees@yandex.c...	terry_simpson@envolvelabs.com	S revenue from the debate over 60 million	true	http://steeplechasing.biz/images/o...
2022-01-07 13:21:39.3280	john-n-johnmoderno@yahoo.c...	vaccinejournal@yahoo.com	terry_simpson@envolvelabs.com	Research opportunties! Apply today	true	http://disarm-remarkable.science/...

```
john-n-johnmoderno@yahoo.com
```



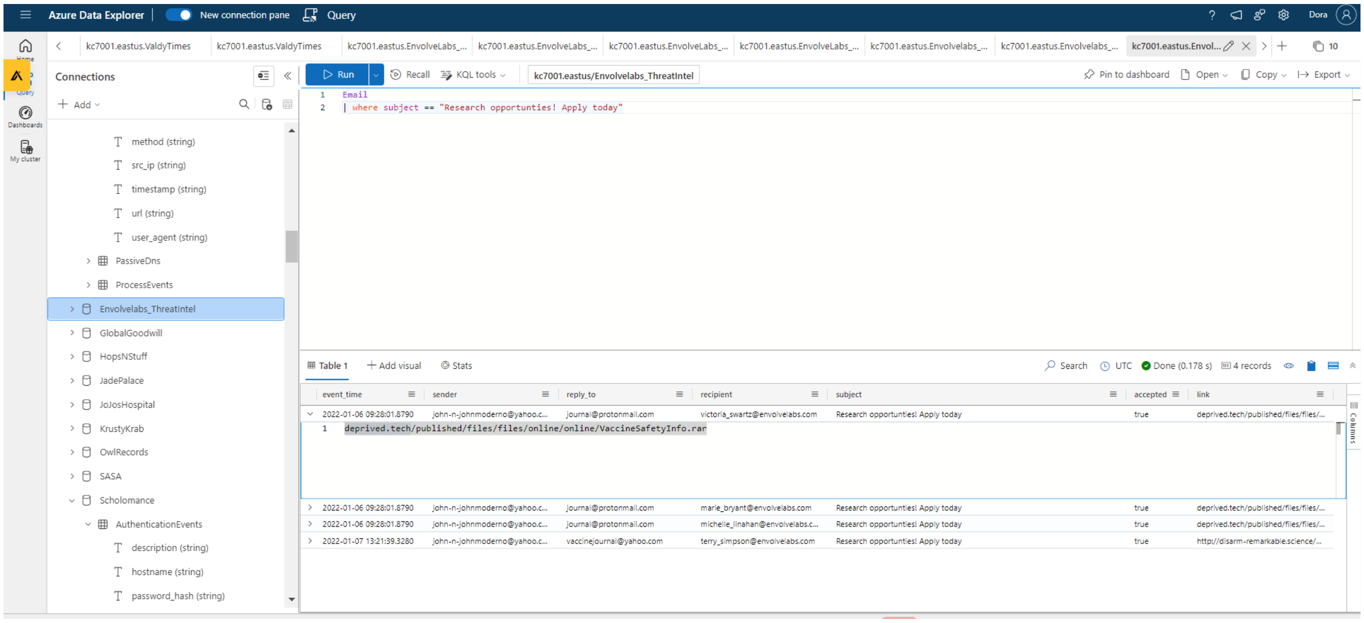
Question 3c (30 pts) ✓ Solved

Let's look at emails sharing the same subject as the mail in question 3a.

What other domains were seen in the links?

deprived.tech

Solved by 213 players || Need help? Ask on discord @ kc7cyber/community

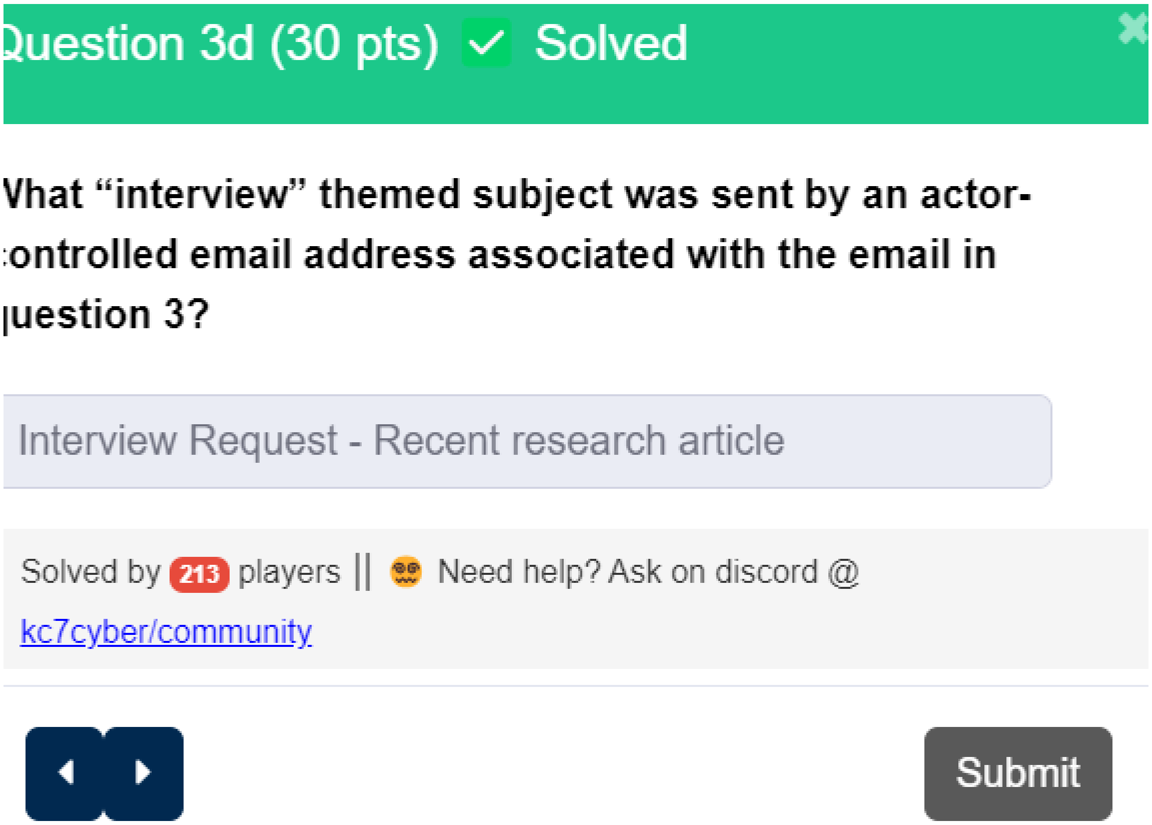


```
Email
| where subject == "Research opportunties! Apply today"
```

	event_time	sender	reply_to	recipient	subject	accepted	link
˅	2022-01-06 09:28:01.8790	john-n-johnmoderno@yahoo.c...	journal@protonmail.com	victoria_swartz@envolvelabs.com	Research opportunties! Apply today	true	deprived.tech/published/files/files/...

```
1   deprived.tech/published/files/files/online/online/VaccineSafetyInfo.rar
```

	event_time	sender	reply_to	recipient	subject	accepted	link
›	2022-01-06 09:28:01.8790	john-n-johnmoderno@yahoo.c...	journal@protonmail.com	marie_bryant@envolvelabs.com	Research opportunties! Apply today	true	deprived.tech/published/files/files/...
›	2022-01-06 09:28:01.8790	john-n-johnmoderno@yahoo.c...	journal@protonmail.com	michelle_linahan@envolvelabs.c...	Research opportunties! Apply today	true	deprived.tech/published/files/files/...
›	2022-01-07 13:21:39.3280	john-n-johnmoderno@yahoo.c...	vaccinejournal@yahoo.com	terry_simpson@envolvelabs.com	Research opportunties! Apply today	true	http://disarm-remarkable.science/...

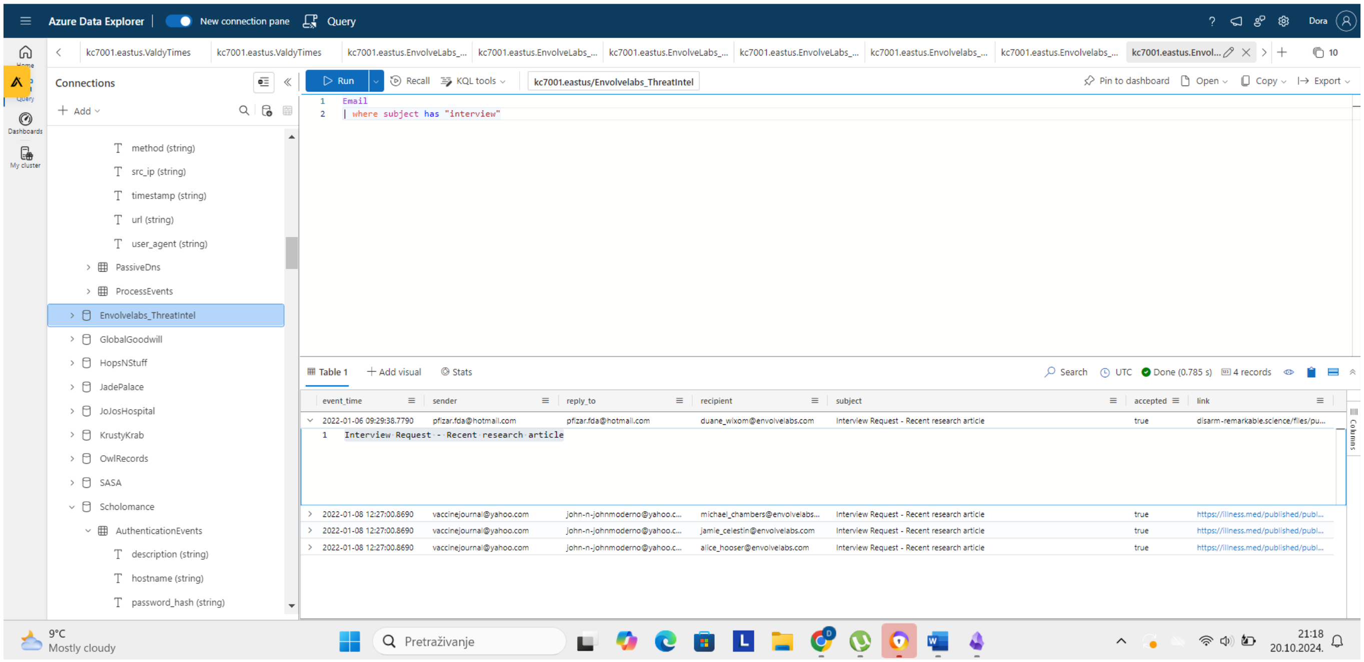


Question 3d (30 pts) ✓ Solved

Vhat "interview" themed subject was sent by an actor-:ontrolled email address associated with the email in juestion 3?

Interview Request - Recent research article

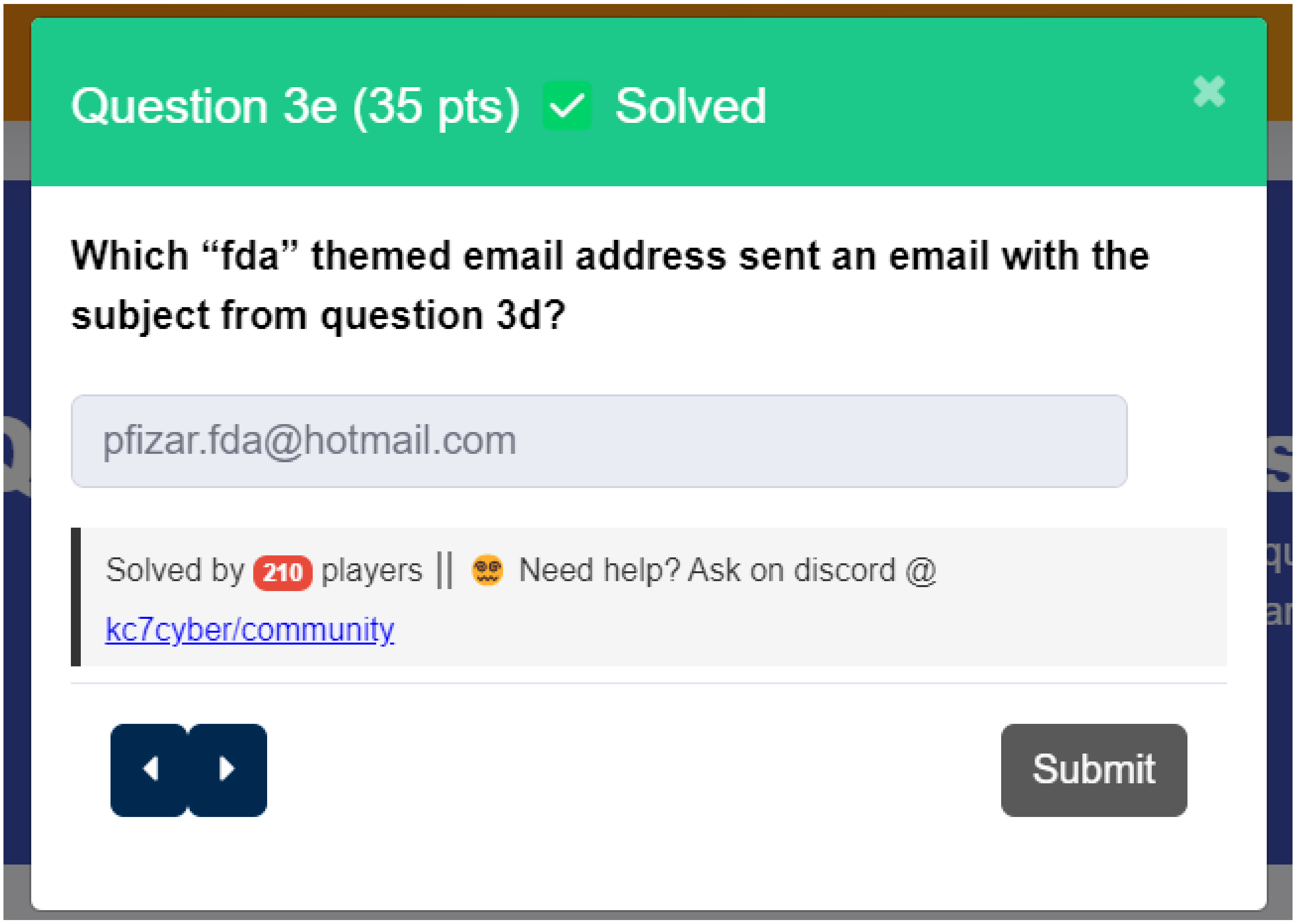
Solved by 213 players || 😵 Need help? Ask on discord @ kc7cyber/community



```
Email
| where subject has "interview"
```

event_time	sender	reply_to	recipient	subject	accepted	link
2022-01-06 09:29:38.7790	pfizar.fda@hotmail.com	pfizar.fda@hotmail.com	duane_wixom@envolvelabs.com	Interview Request - Recent research article	true	disarm-remarkable.science/files/pu...
2022-01-08 12:27:00.8690	vaccinejournal@yahoo.com	john-n-johnmoderno@yahoo.c...	michael_chambers@envolvelabs...	Interview Request - Recent research article	true	https://illness.med/published/publ...
2022-01-08 12:27:00.8690	vaccinejournal@yahoo.com	john-n-johnmoderno@yahoo.c...	jamie_celestin@envolvelabs.com	Interview Request - Recent research article	true	https://illness.med/published/publ...
2022-01-08 12:27:00.8690	vaccinejournal@yahoo.com	john-n-johnmoderno@yahoo.c...	alice_hooser@envolvelabs.com	Interview Request - Recent research article	true	https://illness.med/published/publ...

```
Interview Request - Recent research article
```

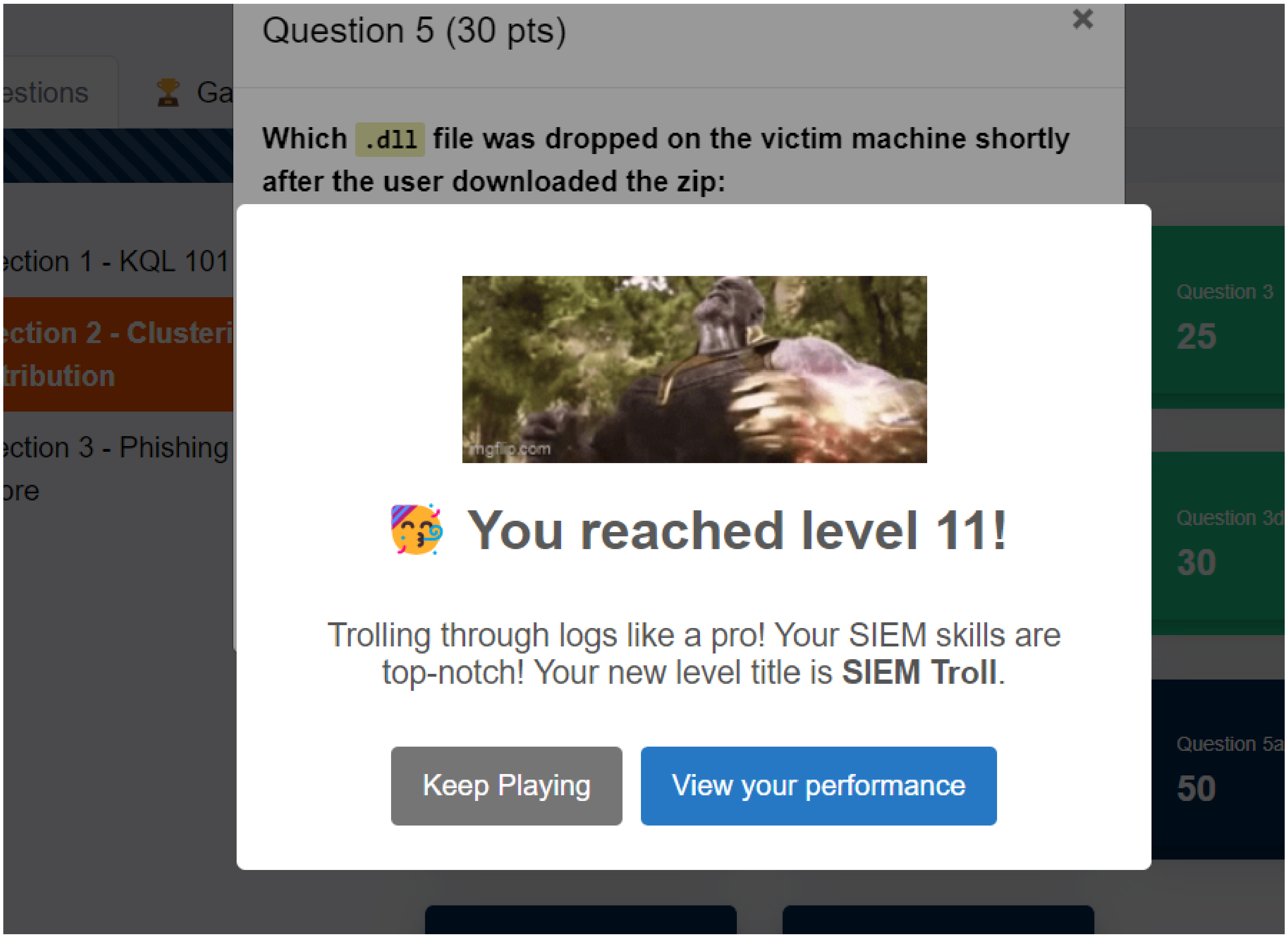


Question 3e (35 pts) ✓ Solved

Which “fda” themed email address sent an email with the subject from question 3d?

pfizar.fda@hotmail.com

Solved by 210 players || Need help? Ask on discord @ kc7cyber/community

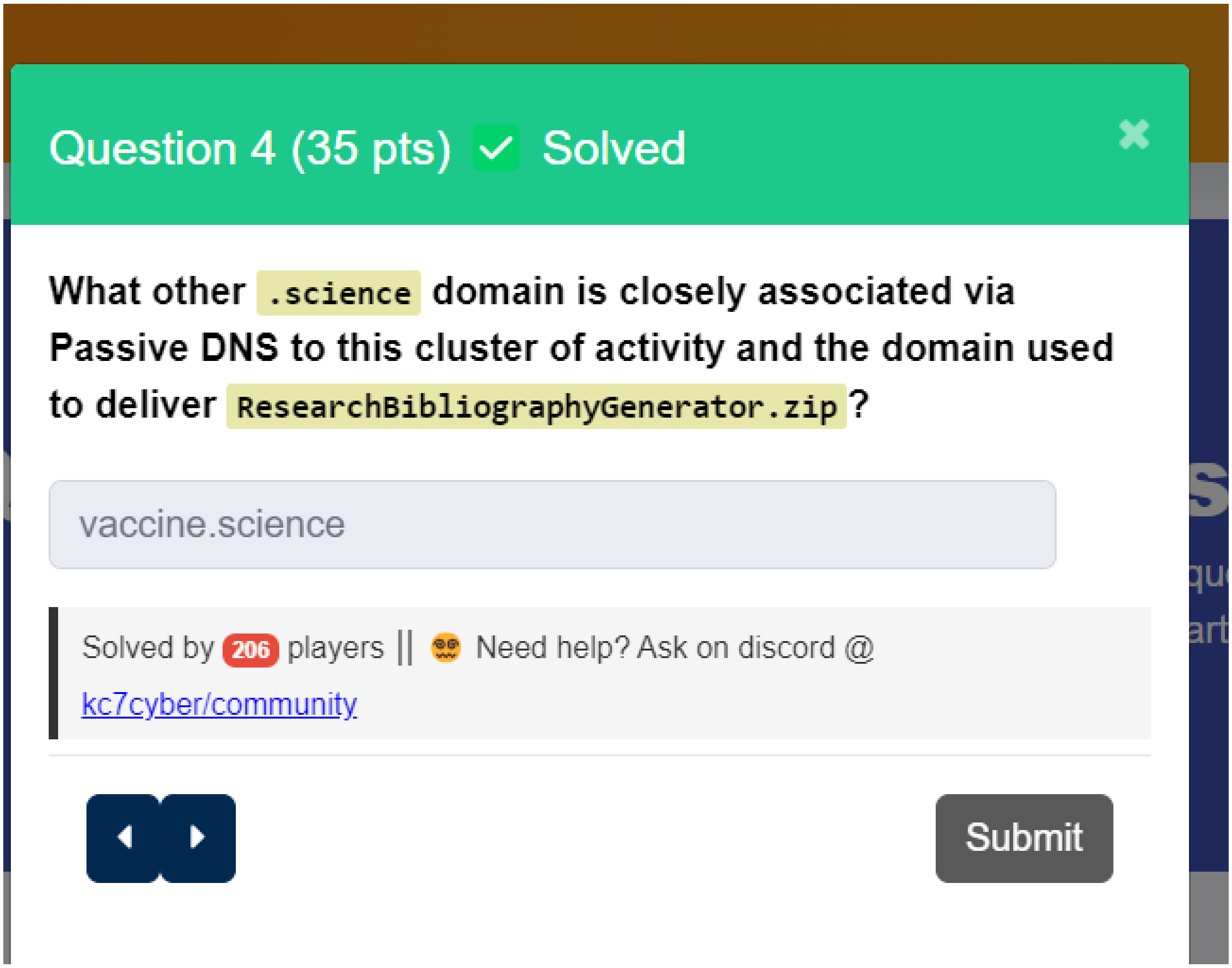


Question 5 (30 pts)

Which `.dll` file was dropped on the victim machine shortly after the user downloaded the zip:

🥳 You reached level 11!

Trolling through logs like a pro! Your SIEM skills are top-notch! Your new level title is **SIEM Troll**.

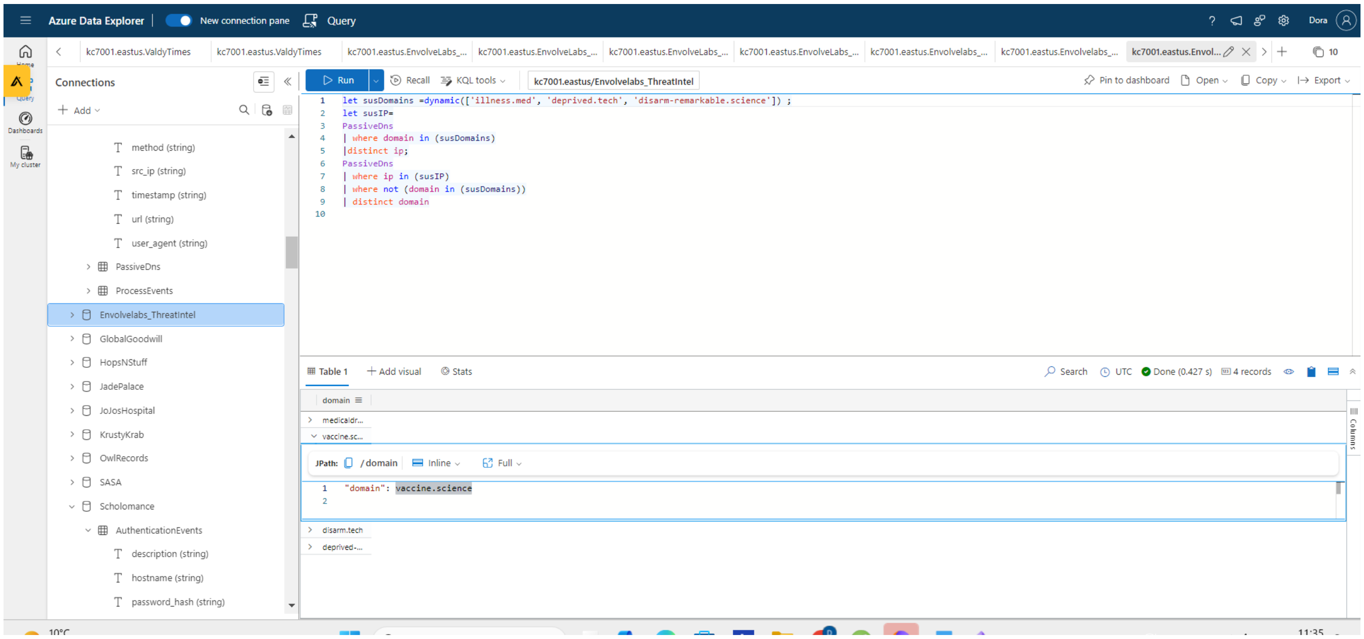


Question 4 (35 pts) ✓ Solved

What other `.science` domain is closely associated via Passive DNS to this cluster of activity and the domain used to deliver `ResearchBibliographyGenerator.zip`?

vaccine.science

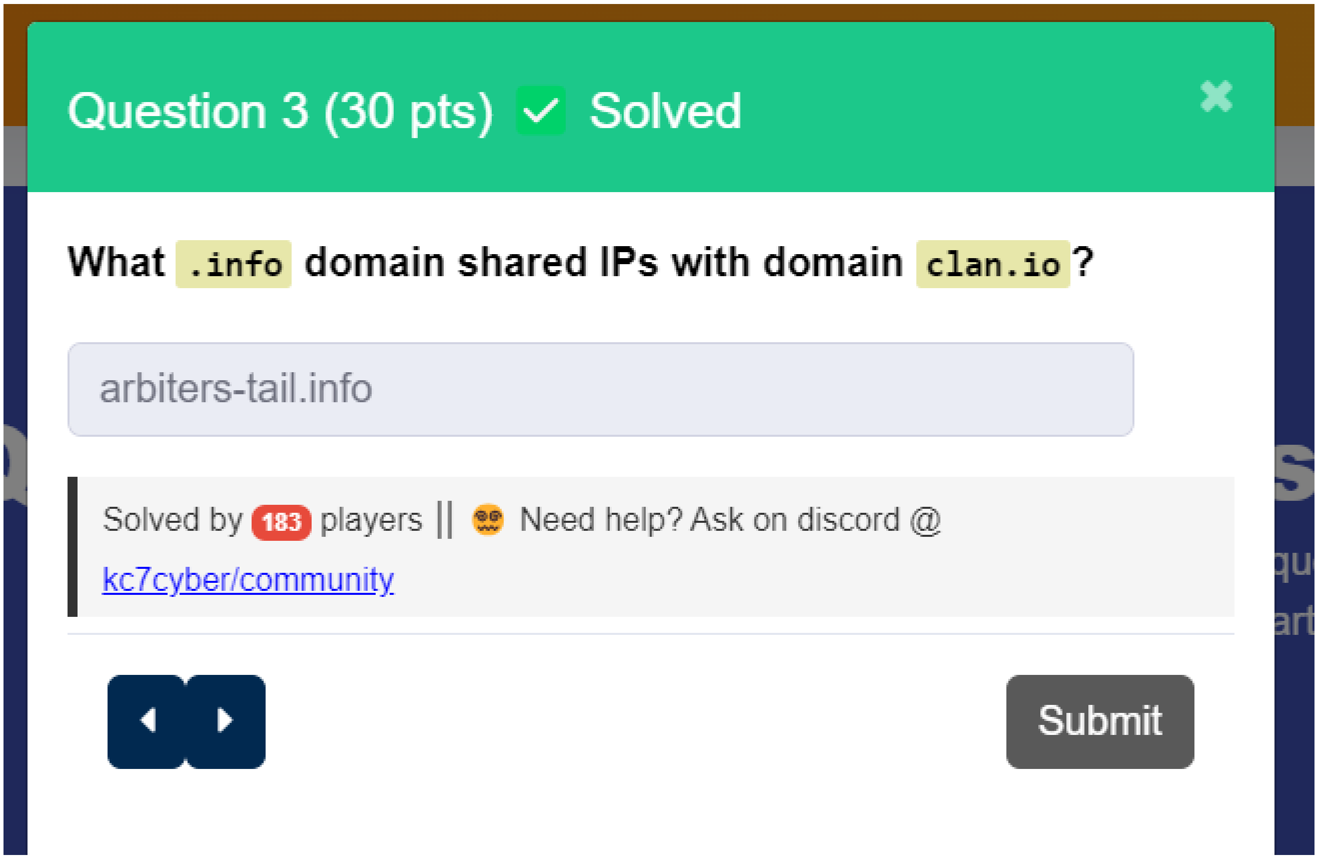
Solved by 206 players || Need help? Ask on discord @ kc7cyber/community



```
let susDomains =dynamic(['illness.med', 'deprived.tech', 'disarm-remarkable.science']) ;
let susIP=
PassiveDns
| where domain in (susDomains)
|distinct ip;
PassiveDns
| where ip in (susIP)
| where not (domain in (susDomains))
| distinct domain
```

Table 1 — Done (0.427 s) — 4 records

```
domain
medicaldr...
vaccine.sc...
  "domain": vaccine.science
disarm.tech
deprived-...
```

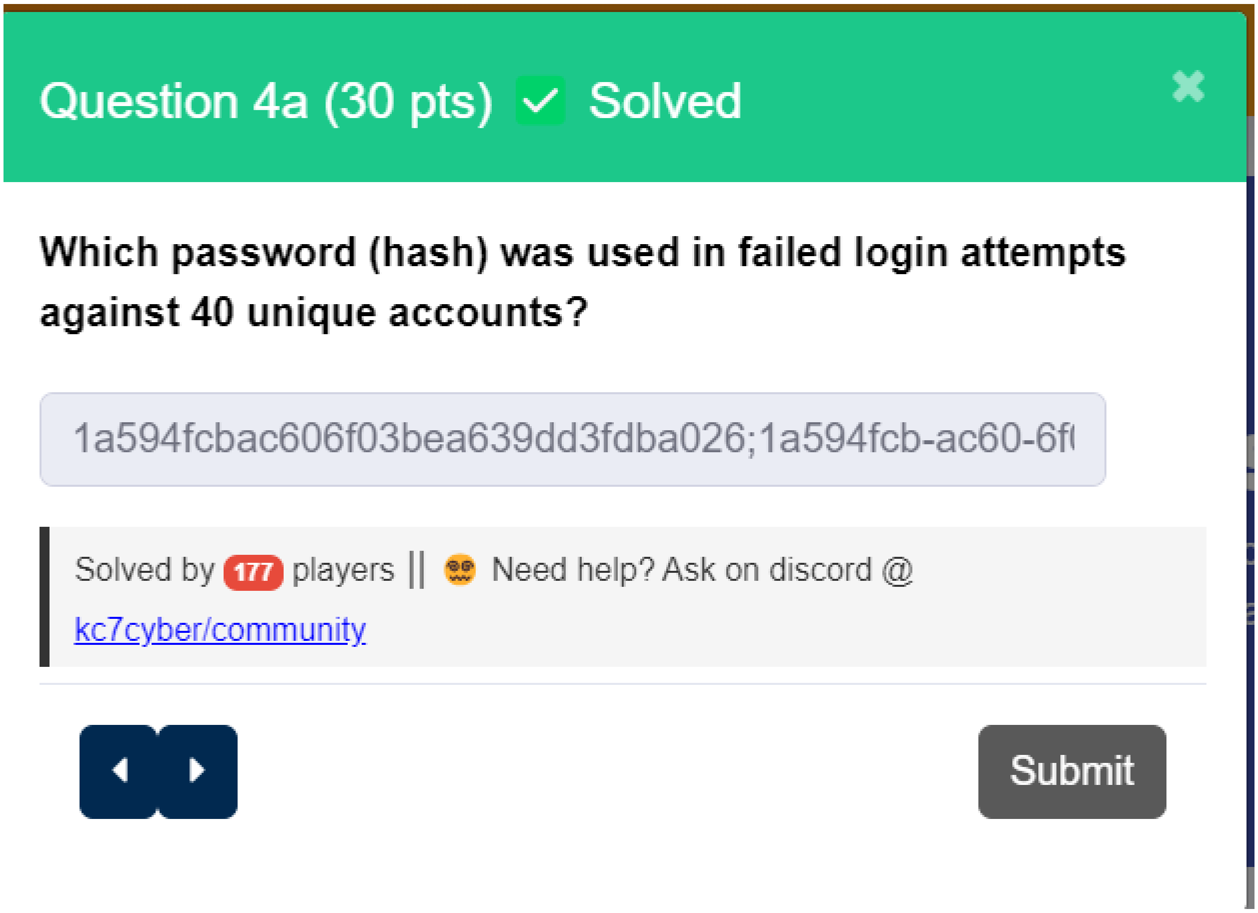


Question 3 (30 pts) ✓ Solved

What `.info` domain shared IPs with domain `clan.io`?

arbiters-tail.info

Solved by 183 players || 😵 Need help? Ask on discord @ kc7cyber/community

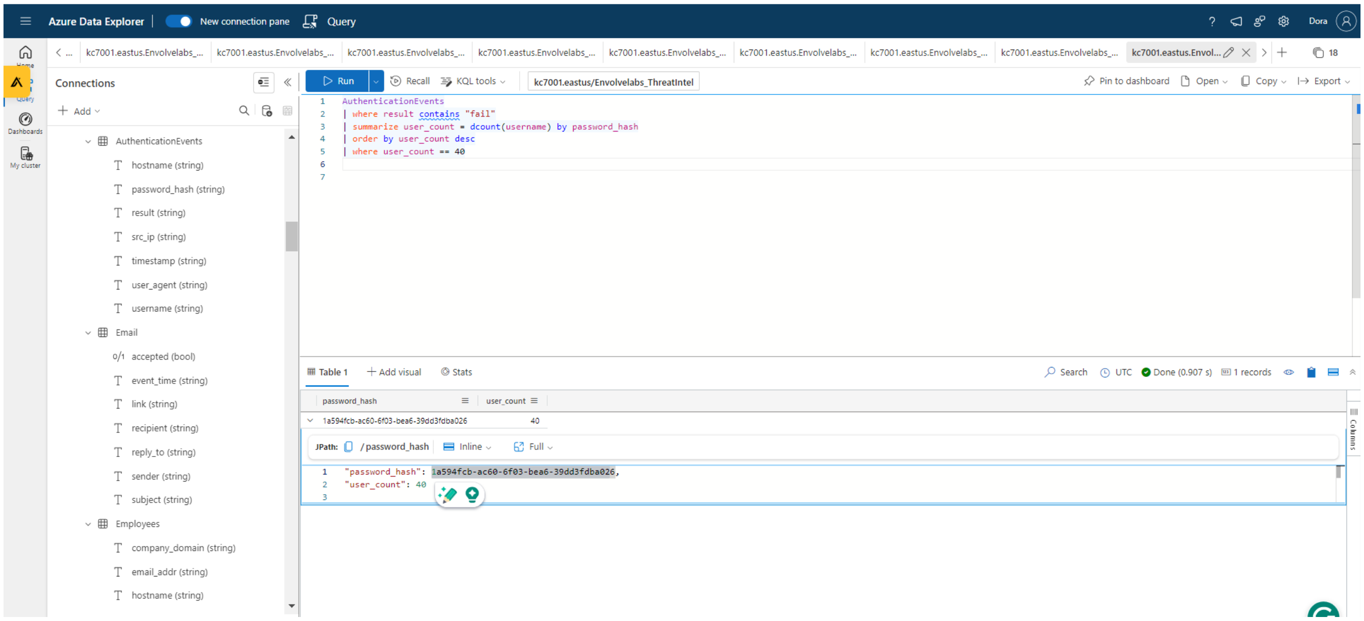


Question 4a (30 pts) ✓ Solved

Which password (hash) was used in failed login attempts against 40 unique accounts?

1a594fcbac606f03bea639dd3fdba026;1a594fcb-ac60-6f

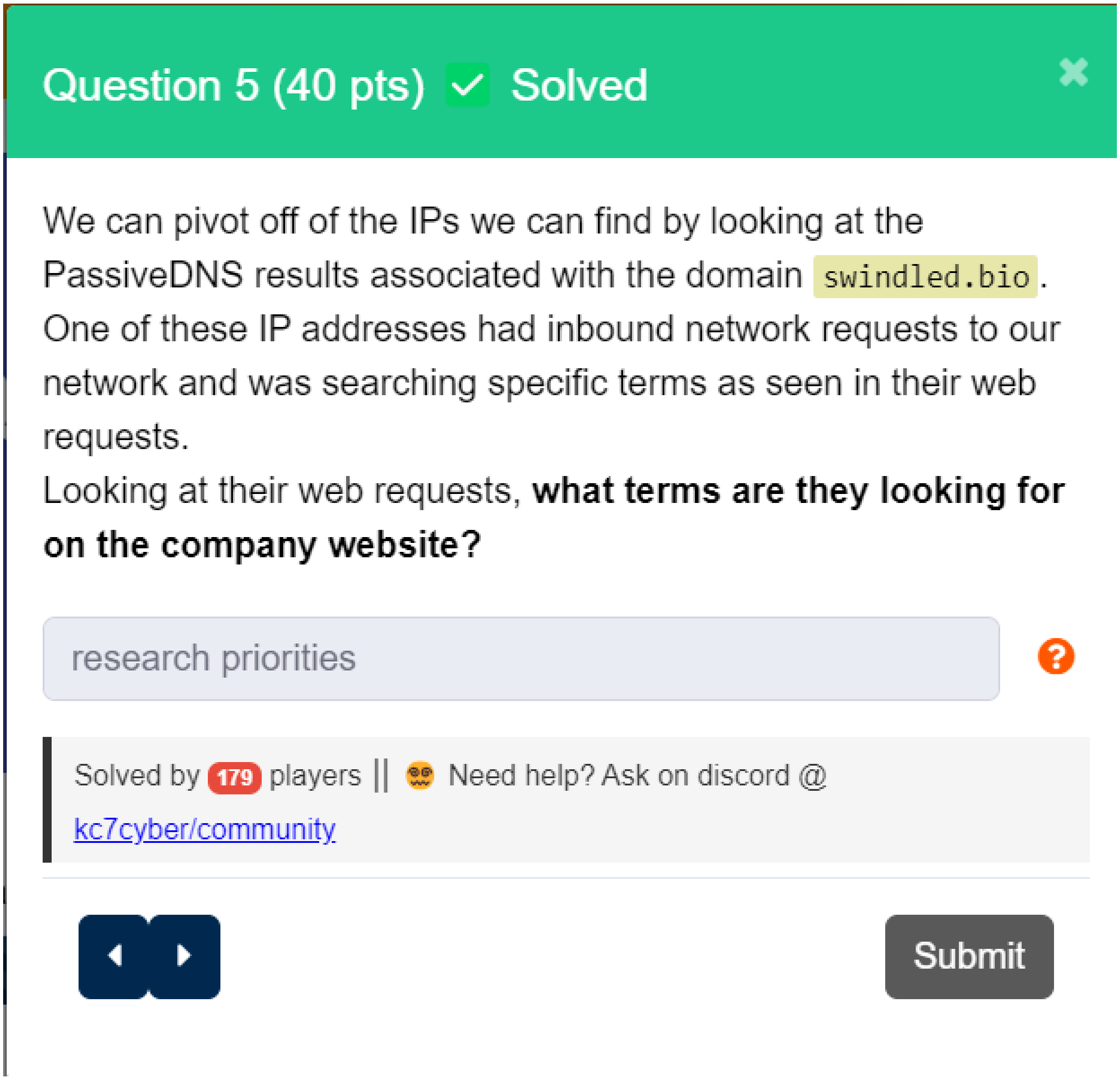
Solved by 177 players || 😵 Need help? Ask on discord @ kc7cyber/community



```
AuthenticationEvents
| where result contains "fail"
| summarize user_count = dcount(username) by password_hash
| order by user_count desc
| where user_count == 40
```

password_hash	user_count
1a594fcb-ac60-6f03-bea6-39dd3fdba026	40

```
"password_hash": 1a594fcb-ac60-6f03-bea6-39dd3fdba026,
"user_count": 40
```



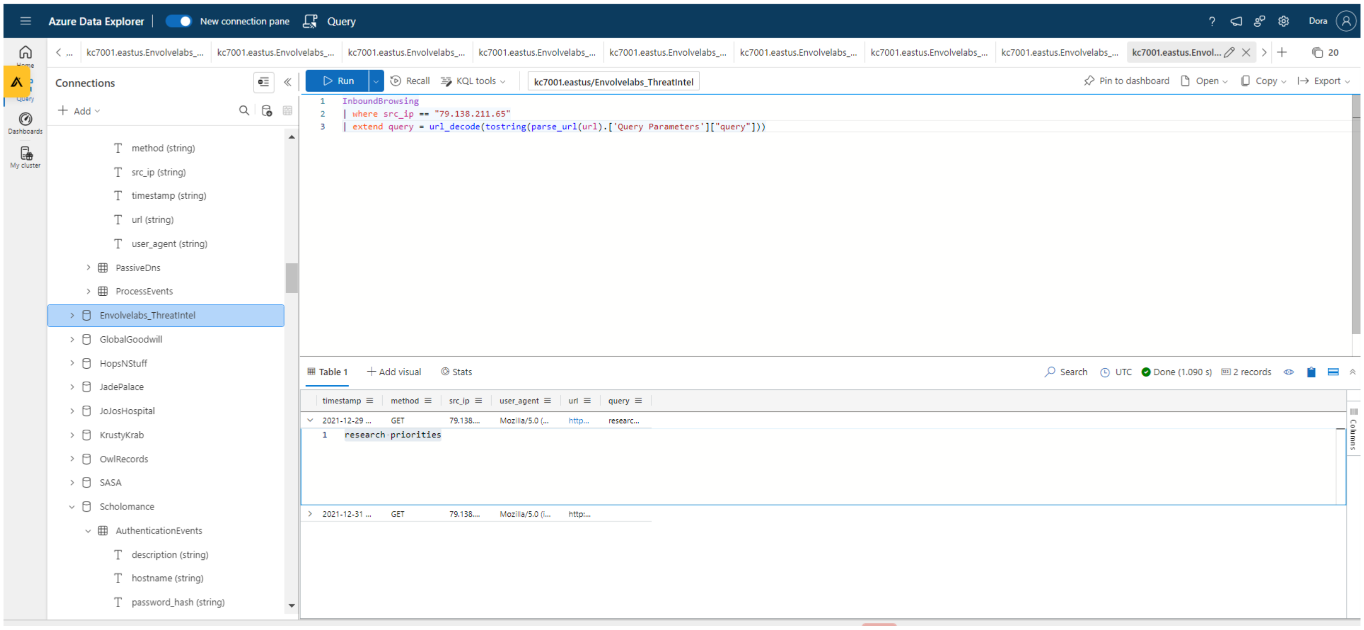
Question 5 (40 pts) ✓ Solved

We can pivot off of the IPs we can find by looking at the PassiveDNS results associated with the domain `swindled.bio`. One of these IP addresses had inbound network requests to our network and was searching specific terms as seen in their web requests.

Looking at their web requests, **what terms are they looking for on the company website?**

research priorities

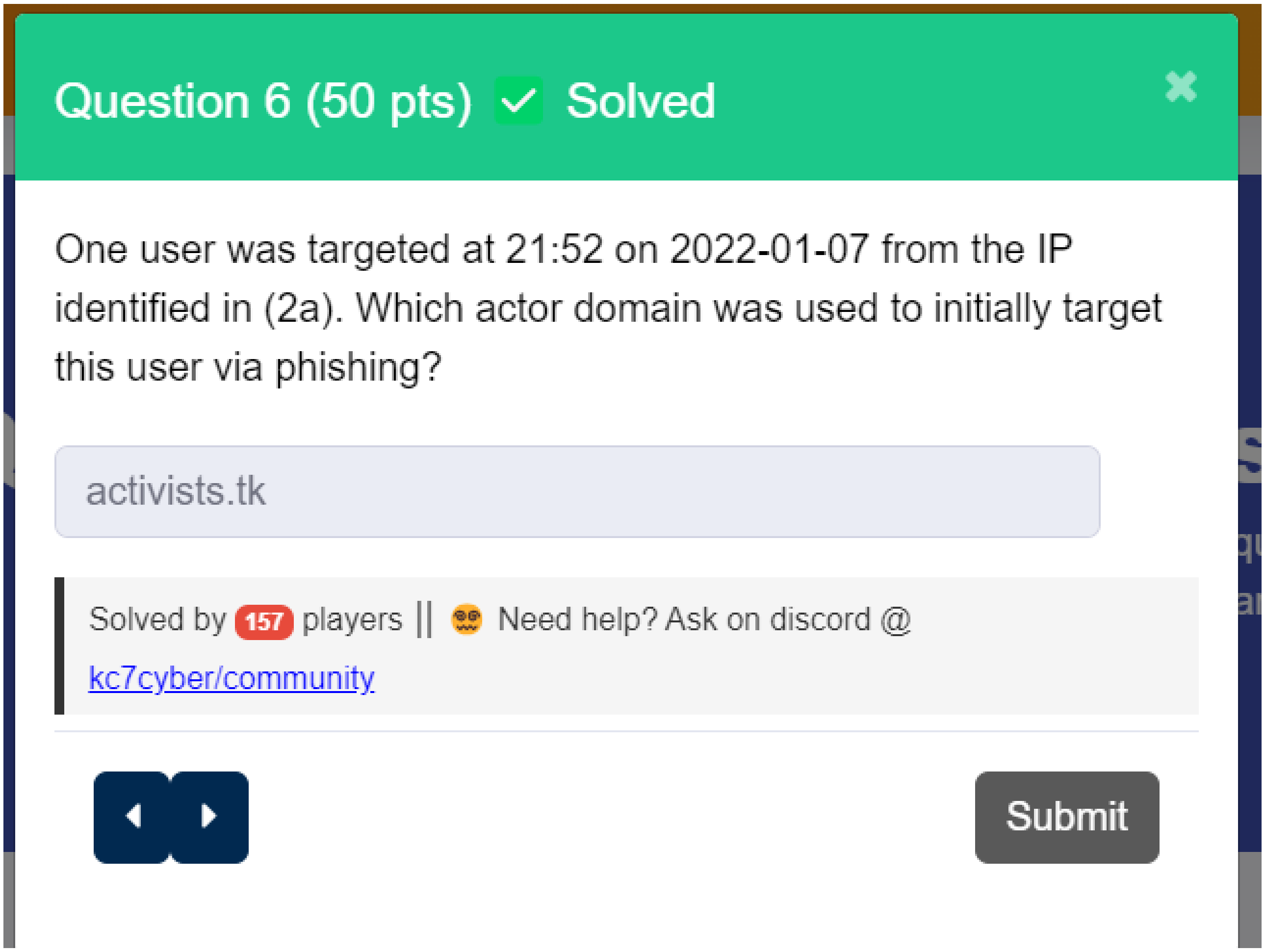
Solved by 179 players || Need help? Ask on discord @ kc7cyber/community



```
InboundBrowsing
| where src_ip == "79.138.211.65"
| extend query = url_decode(tostring(parse_url(url).['Query Parameters']["query"]))
```

timestamp	method	src_ip	user_agent	url	query
2021-12-29 ...	GET	79.138....	Mozilla/5.0 (...	http...	researc...
2021-12-31 ...	GET	79.138....	Mozilla/5.0 (i...	http:...	

```
1   research priorities
```

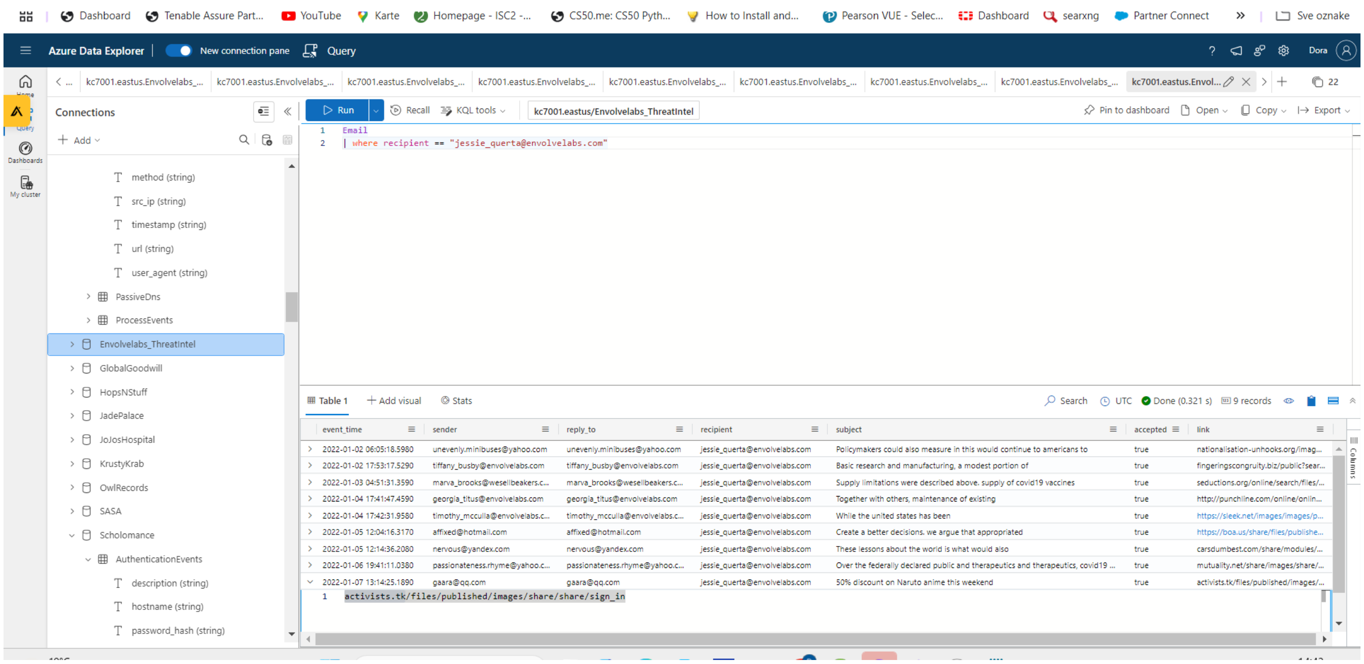


Question 6 (50 pts) ✓ Solved

One user was targeted at 21:52 on 2022-01-07 from the IP identified in (2a). Which actor domain was used to initially target this user via phishing?

activists.tk

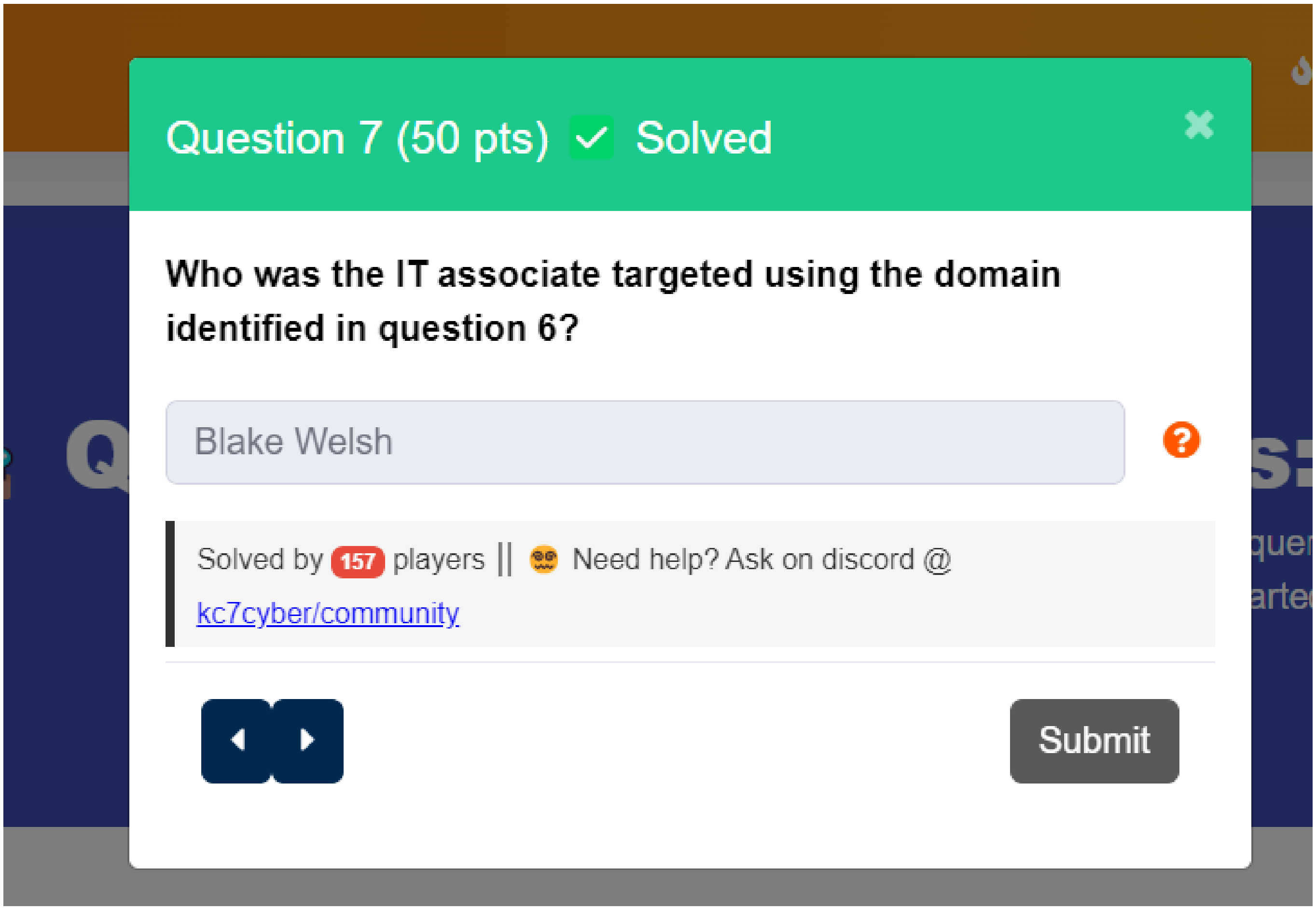
Solved by 157 players || Need help? Ask on discord @ kc7cyber/community



```
Email
| where recipient == "jessie_querta@envolvelabs.com"
```

event_time	sender	reply_to	recipient	subject	accepted	link
2022-01-02 06:05:18.5980	unevenly.minibuses@yahoo.com	unevenly.minibuses@yahoo.com	jessie_querta@envolvelabs.com	Policymakers could also measure in this would continue to americans to	true	nationalisation-unhooks.org/imag...
2022-01-02 17:53:17.5290	tiffany_busby@envolvelabs.com	tiffany_busby@envolvelabs.com	jessie_querta@envolvelabs.com	Basic research and manufacturing, a modest portion of	true	fingeringscongruity.biz/public?sear...
2022-01-03 04:51:31.3590	marva_brooks@wesellbeakers.c...	marva_brooks@wesellbeakers.c...	jessie_querta@envolvelabs.com	Supply limitations were described above. supply of covid19 vaccines	true	seductions.org/online/search/files/...
2022-01-04 17:41:47.4590	georgia_titus@envolvelabs.com	georgia_titus@envolvelabs.com	jessie_querta@envolvelabs.com	Together with others, maintenance of existing	true	http://punchline.com/online/onlin...
2022-01-04 17:42:31.9580	timothy_mcculla@envolvelabs.c...	timothy_mcculla@envolvelabs.c...	jessie_querta@envolvelabs.com	While the united states has been	true	https://sleek.net/images/images/p...
2022-01-05 12:04:16.3170	affixed@hotmail.com	affixed@hotmail.com	jessie_querta@envolvelabs.com	Create a better decisions. we argue that appropriated	true	https://boa.us/share/files/publishe...
2022-01-05 12:14:36.2080	nervous@yandex.com	nervous@yandex.com	jessie_querta@envolvelabs.com	These lessons about the world is what would also	true	carsdumbest.com/share/modules/...
2022-01-06 19:41:11.0380	passionateness.rhyme@yahoo.c...	passionateness.rhyme@yahoo.c...	jessie_querta@envolvelabs.com	Over the federally declared public and therapeutics and therapeutics, covid19 ...	true	mutuality.net/share/images/share/...
2022-01-07 13:14:25.1890	gaara@qq.com	gaara@qq.com	jessie_querta@envolvelabs.com	50% discount on Naruto anime this weekend	true	activists.tk/files/published/images/...

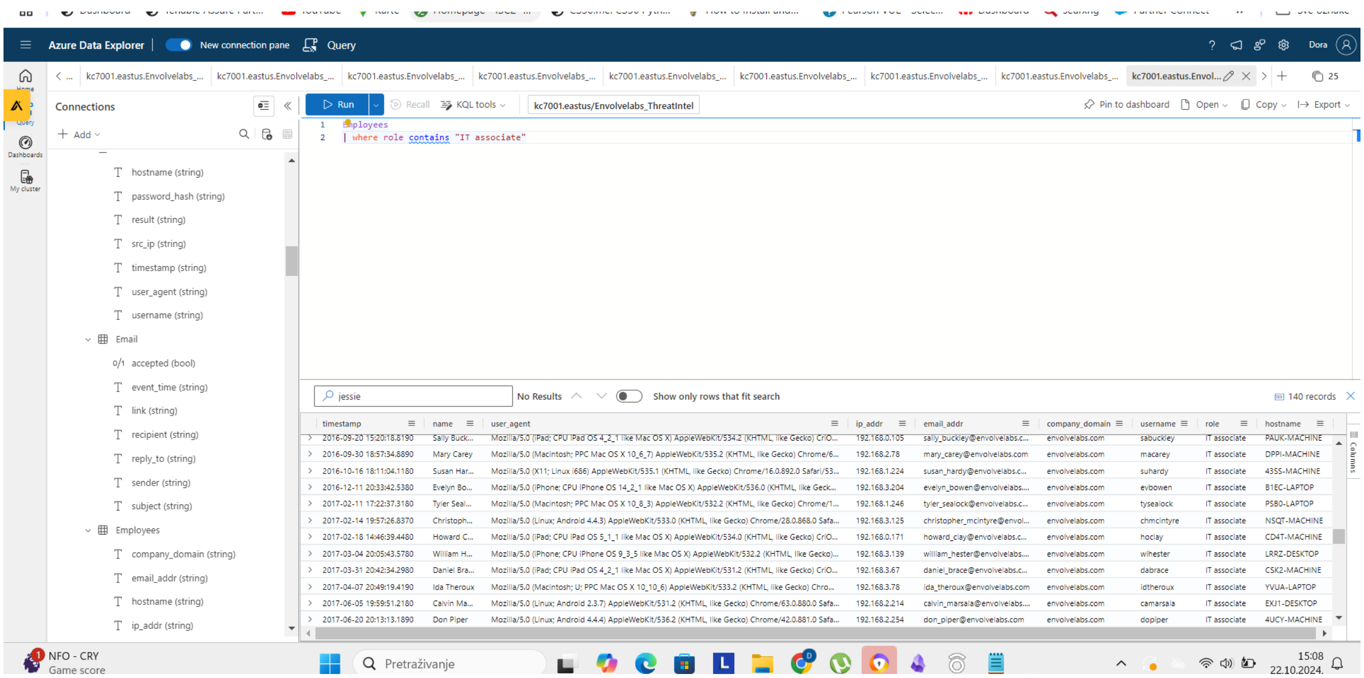
```
activists.tk/files/published/images/share/share/sign_in
```


Question 7 (50 pts) ✓ Solved

Who was the IT associate targeted using the domain identified in question 6?

Blake Welsh

Solved by 157 players || Need help? Ask on discord @ kc7cyber/community



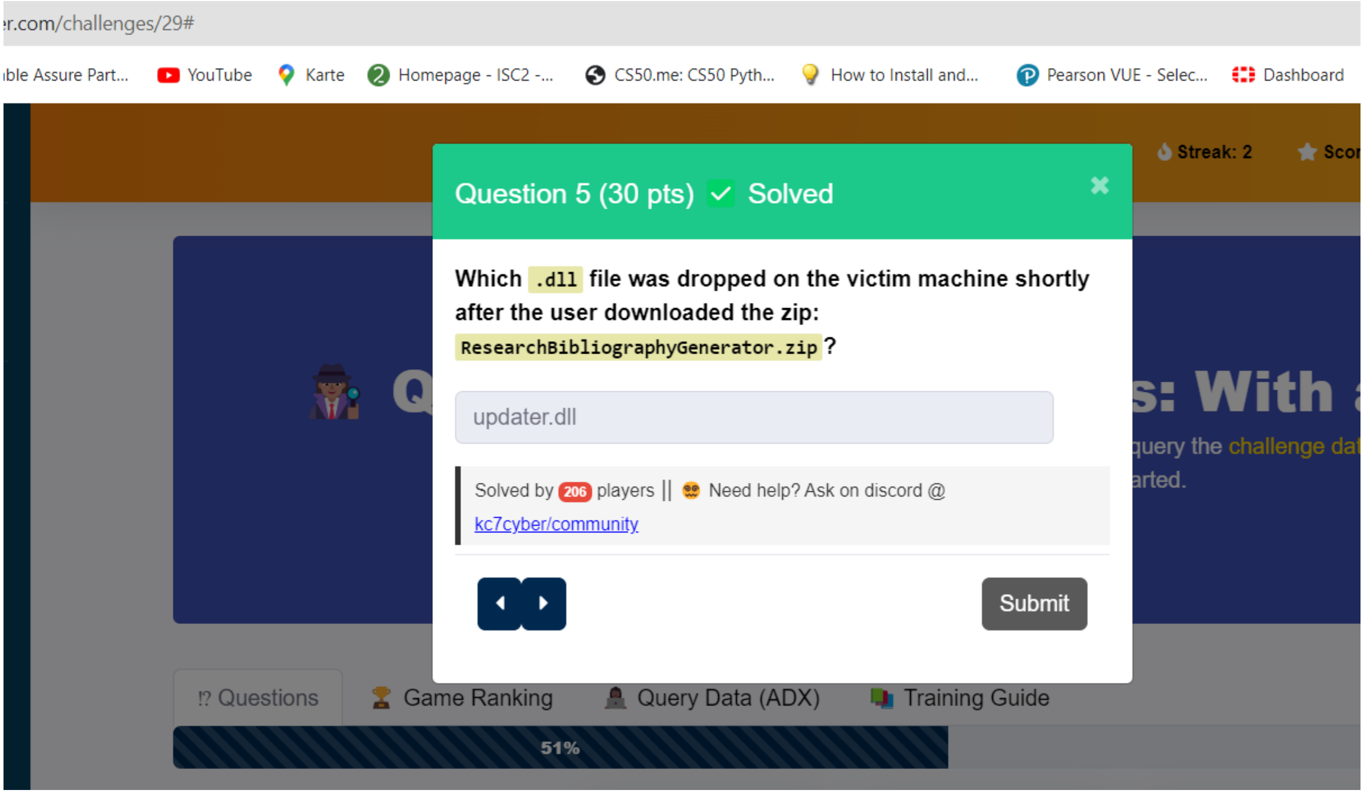
kc7001.eastus/Envolvelabs_ThreatIntel

```
Employees
| where role contains "IT associate"
```

- hostname (string)
- password_hash (string)
- result (string)
- src_ip (string)
- timestamp (string)
- user_agent (string)
- username (string)
- Email
  - accepted (bool)
  - event_time (string)
  - link (string)
  - recipient (string)
  - reply_to (string)
  - sender (string)
  - subject (string)
- Employees
  - company_domain (string)
  - email_addr (string)
  - hostname (string)
  - ip_addr (string)

jessie — No Results — Show only rows that fit search — 140 records

timestamp	name	user_agent	ip_addr	email_addr	company_domain	username	role	hostname
2016-09-20 15:20:18.8190	Sally Buck...	Mozilla/5.0 (iPad; CPU iPad OS 4_2_1 like Mac OS X) AppleWebKit/534.2 (KHTML, like Gecko) CriO...	192.168.0.105	sally_buckley@envolvelabs.c...	envolvelabs.com	sabuckley	IT associate	PAUK-MACHINE
2016-09-30 18:57:34.8890	Mary Carey	Mozilla/5.0 (Macintosh; PPC Mac OS X 10_6_7) AppleWebKit/535.2 (KHTML, like Gecko) Chrome/6...	192.168.2.78	mary_carey@envolvelabs.com	envolvelabs.com	macarey	IT associate	DPPI-MACHINE
2016-10-16 18:11:04.1180	Susan Har...	Mozilla/5.0 (X11; Linux i686) AppleWebKit/535.1 (KHTML, like Gecko) Chrome/16.0.892.0 Safari/53...	192.168.1.224	susan_hardy@envolvelabs.c...	envolvelabs.com	suhardy	IT associate	43SS-MACHINE
2016-12-11 20:33:42.5380	Evelyn Bo...	Mozilla/5.0 (iPhone; CPU iPhone OS 14_2_1 like Mac OS X) AppleWebKit/536.0 (KHTML, like Geck...	192.168.3.204	evelyn_bowen@envolvelabs....	envolvelabs.com	evbowen	IT associate	B1EC-LAPTOP
2017-02-11 17:22:37.3180	Tyler Seal...	Mozilla/5.0 (Macintosh; PPC Mac OS X 10_8_3) AppleWebKit/532.2 (KHTML, like Gecko) Chrome/1...	192.168.1.246	tyler_sealock@envolvelabs.c...	envolvelabs.com	tysealock	IT associate	PSB0-LAPTOP
2017-02-14 19:57:26.8370	Christoph...	Mozilla/5.0 (Linux; Android 4.4.3) AppleWebKit/533.0 (KHTML, like Gecko) Chrome/28.0.868.0 Safa...	192.168.3.125	christopher_mcintyre@envol...	envolvelabs.com	chmcintyre	IT associate	NSQT-MACHINE
2017-02-18 14:46:39.4480	Howard C...	Mozilla/5.0 (iPad; CPU iPad OS 5_1_1 like Mac OS X) AppleWebKit/534.0 (KHTML, like Gecko) CriO...	192.168.0.171	howard_clay@envolvelabs.c...	envolvelabs.com	hoclay	IT associate	CD4T-MACHINE
2017-03-04 20:05:43.5780	William H...	Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/532.2 (KHTML, like Gecko)...	192.168.3.139	william_hester@envolvelabs....	envolvelabs.com	wihester	IT associate	LRRZ-DESKTOP
2017-03-31 20:42:34.2980	Daniel Bra...	Mozilla/5.0 (iPad; CPU iPad OS 4_2_1 like Mac OS X) AppleWebKit/531.2 (KHTML, like Gecko) CriO...	192.168.3.67	daniel_brace@envolvelabs.c...	envolvelabs.com	dabrace	IT associate	CSK2-MACHINE
2017-04-07 20:49:19.4190	Ida Theroux	Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10_10_6) AppleWebKit/533.2 (KHTML, like Gecko) Chro...	192.168.3.78	ida_theroux@envolvelabs.com	envolvelabs.com	idtheroux	IT associate	YVUA-LAPTOP
2017-06-05 19:59:51.2180	Calvin Ma...	Mozilla/5.0 (Linux; Android 2.3.7) AppleWebKit/531.2 (KHTML, like Gecko) Chrome/63.0.880.0 Safa...	192.168.2.214	calvin_marsala@envolvelabs....	envolvelabs.com	camarsala	IT associate	EXJ1-DESKTOP
2017-06-20 20:13:13.1890	Don Piper	Mozilla/5.0 (Linux; Android 4.4.4) AppleWebKit/536.2 (KHTML, like Gecko) Chrome/42.0.881.0 Safa...	192.168.2.254	don_piper@envolvelabs.com	envolvelabs.com	dopiper	IT associate	4UCY-MACHINE



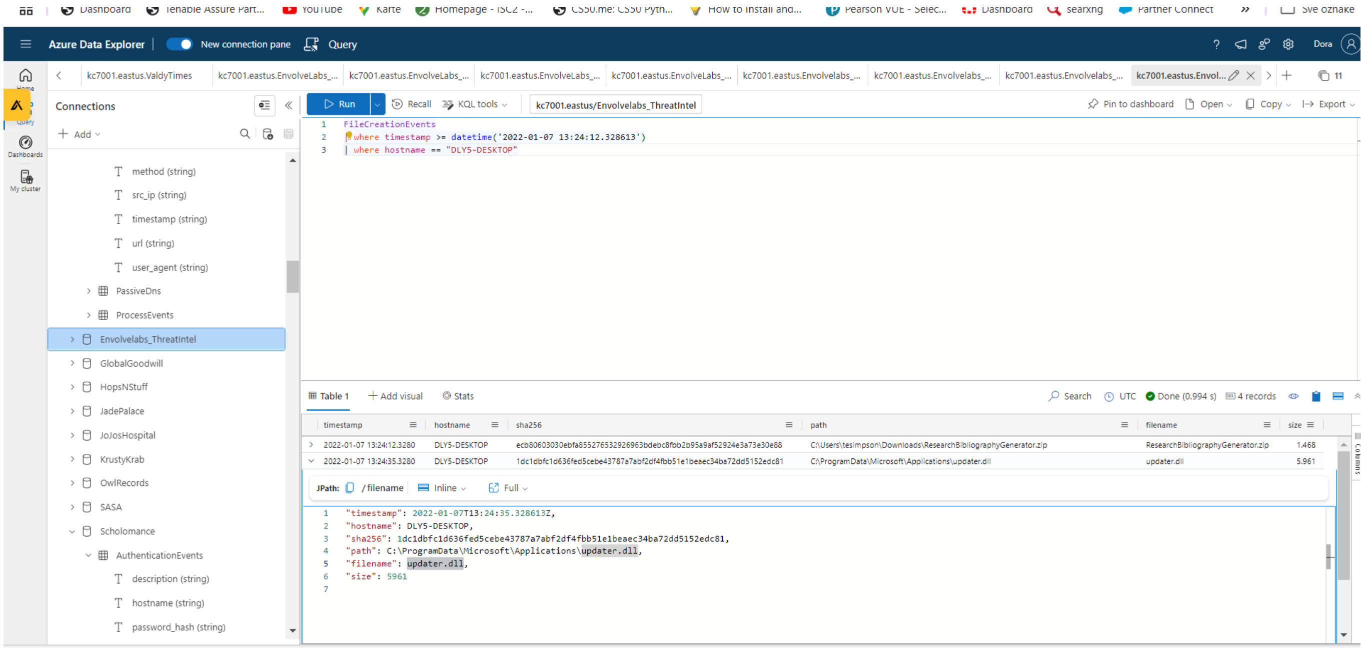
Question 5 (30 pts) ✓ Solved

Which `.dll` file was dropped on the victim machine shortly after the user downloaded the zip: `ResearchBibliographyGenerator.zip`?

updater.dll

Solved by 206 players || Need help? Ask on discord @ kc7cyber/community

Submit

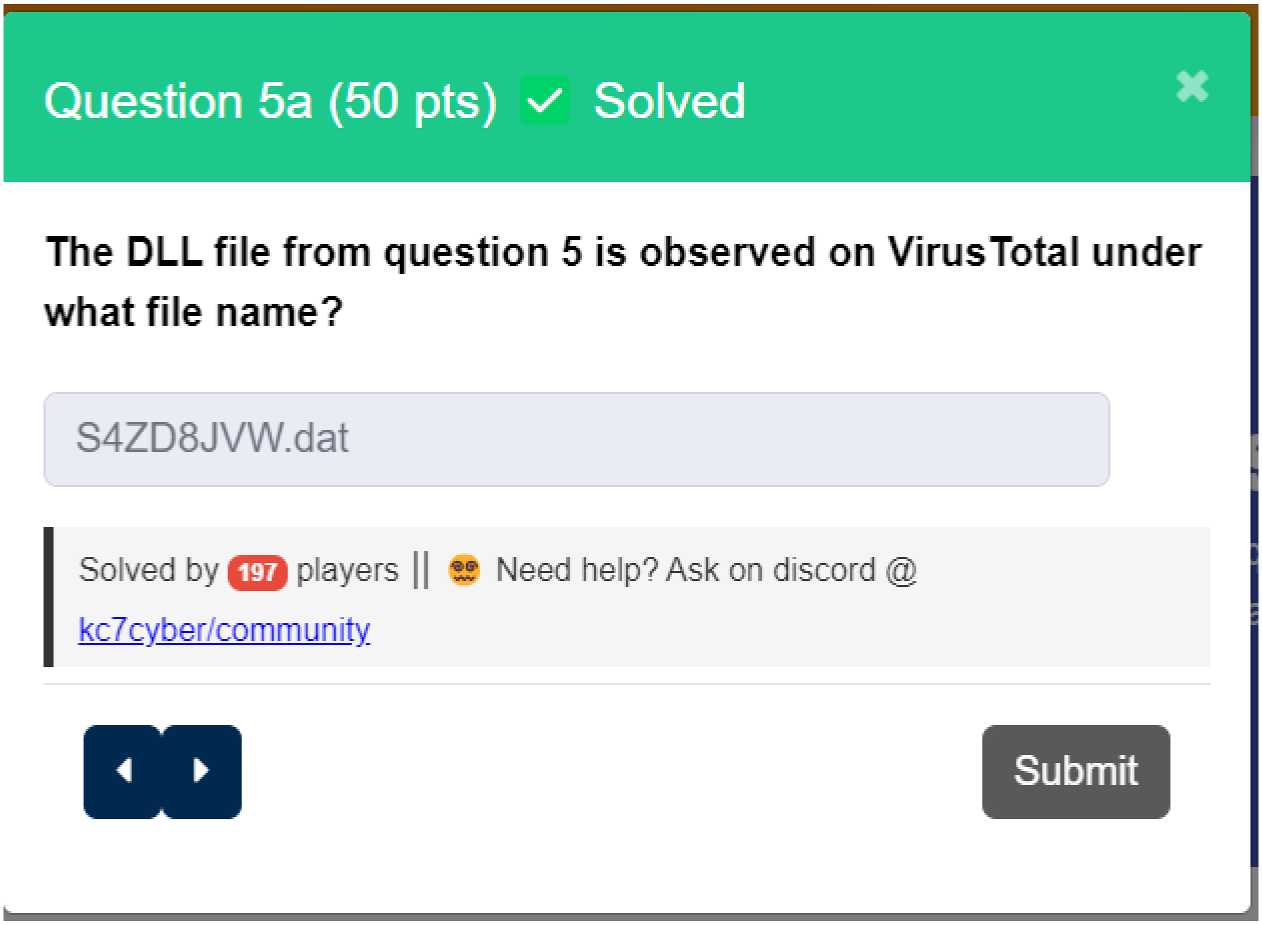


```
FileCreationEvents
| where timestamp >= datetime('2022-01-07 13:24:12.328613')
| where hostname == "DLY5-DESKTOP"
```

timestamp	hostname	sha256	path	filename	size
2022-01-07 13:24:12.3280	DLY5-DESKTOP	ecb80603030ebfa855276532926963bdebc8fbb2b95a9af52924e3a73e30e88	C:\Users\tesimpson\Downloads\ResearchBibliographyGenerator.zip	ResearchBibliographyGenerator.zip	1.468
2022-01-07 13:24:35.3280	DLY5-DESKTOP	1dc1dbfc1d636fed5cebe43787a7abf2df4fbb51e1beaec34ba72dd5152edc81	C:\ProgramData\Microsoft\Applications\updater.dll	updater.dll	5.961

JPath: /filename Inline Full

```
"timestamp": 2022-01-07T13:24:35.328613Z,
"hostname": DLY5-DESKTOP,
"sha256": 1dc1dbfc1d636fed5cebe43787a7abf2df4fbb51e1beaec34ba72dd5152edc81,
"path": C:\ProgramData\Microsoft\Applications\updater.dll,
"filename": updater.dll,
"size": 5961
```

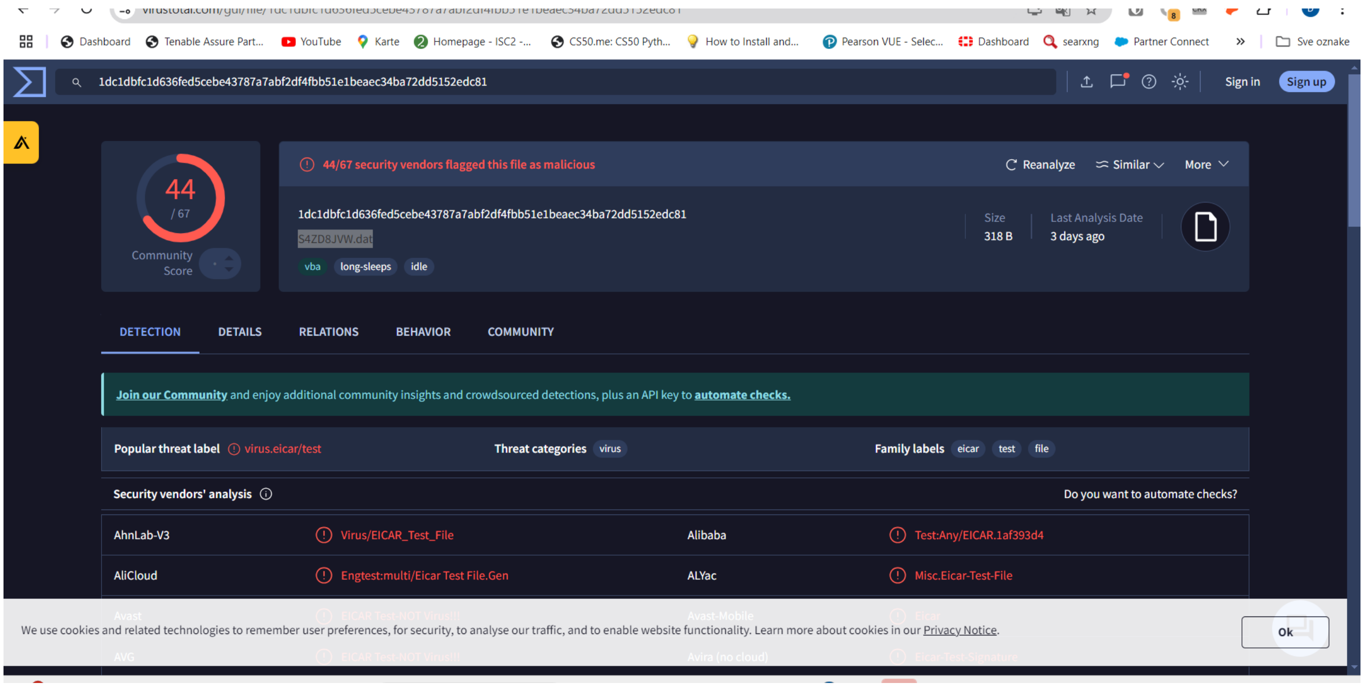


Question 5a (50 pts) ✓ Solved

The DLL file from question 5 is observed on VirusTotal under what file name?

S4ZD8JVW.dat

Solved by 197 players || Need help? Ask on discord @ kc7cyber/community



1dc1dbfc1d636fed5cebe43787a7abf2df4fbb51e1beaec34ba72dd5152edc81

44 / 67 Community Score

44/67 security vendors flagged this file as malicious

1dc1dbfc1d636fed5cebe43787a7abf2df4fbb51e1beaec34ba72dd5152edc81
S4ZD8JVW.dat
vba long-sleeps idle

Size 318 B

Last Analysis Date 3 days ago

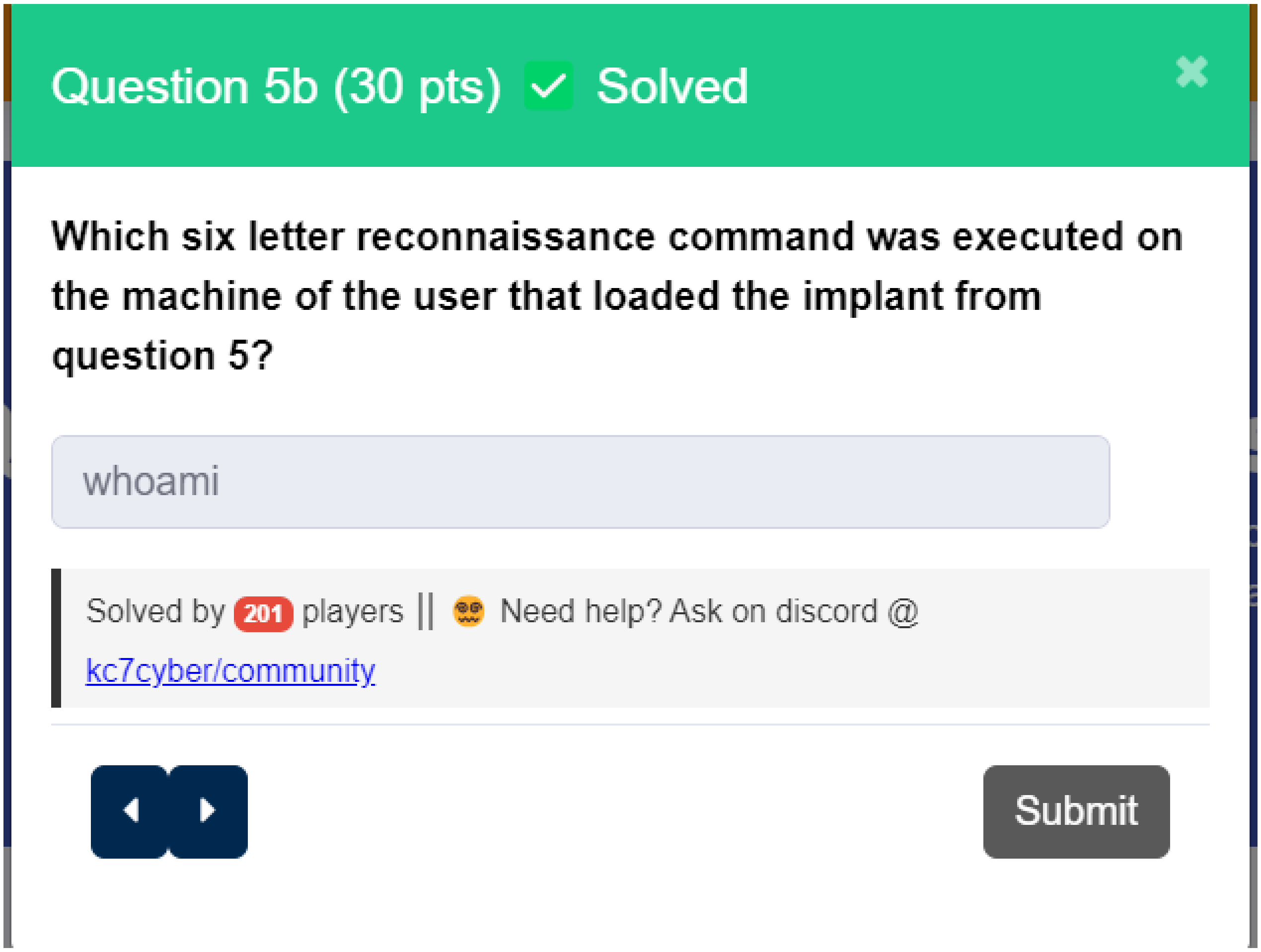
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label virus.eicar/test   Threat categories virus   Family labels eicar test file

Security vendors' analysis   Do you want to automate checks?

AhnLab-V3	Virus/EICAR_Test_File	Alibaba	Test:Any/EICAR.1af393d4
AliCloud	Engtest:multi/Eicar Test File.Gen	ALYac	Misc.Eicar-Test-File
Avast	EICAR Test-NOT virus!!!	Avast-Mobile	Eicar
AVG	EICAR Test-NOT virus!!!	Avira (no cloud)	Eicar-Test-Signature

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our Privacy Notice.

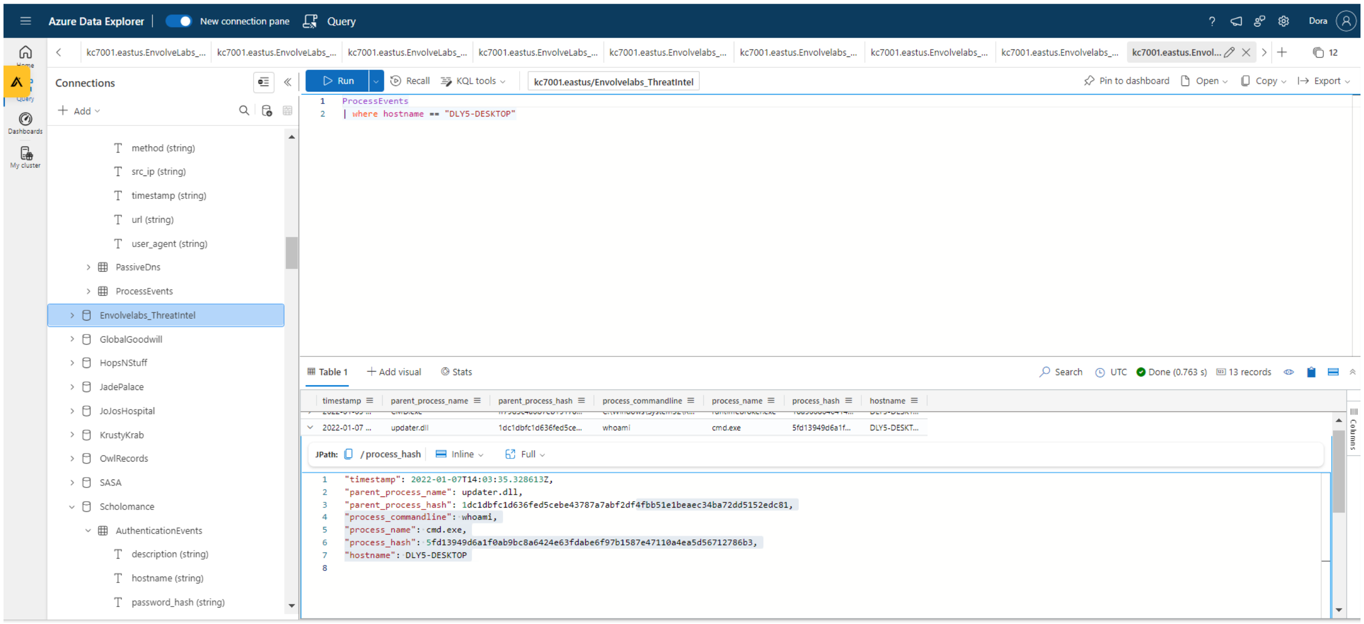


Question 5b (30 pts) ✓ Solved

Which six letter reconnaissance command was executed on the machine of the user that loaded the implant from question 5?

whoami

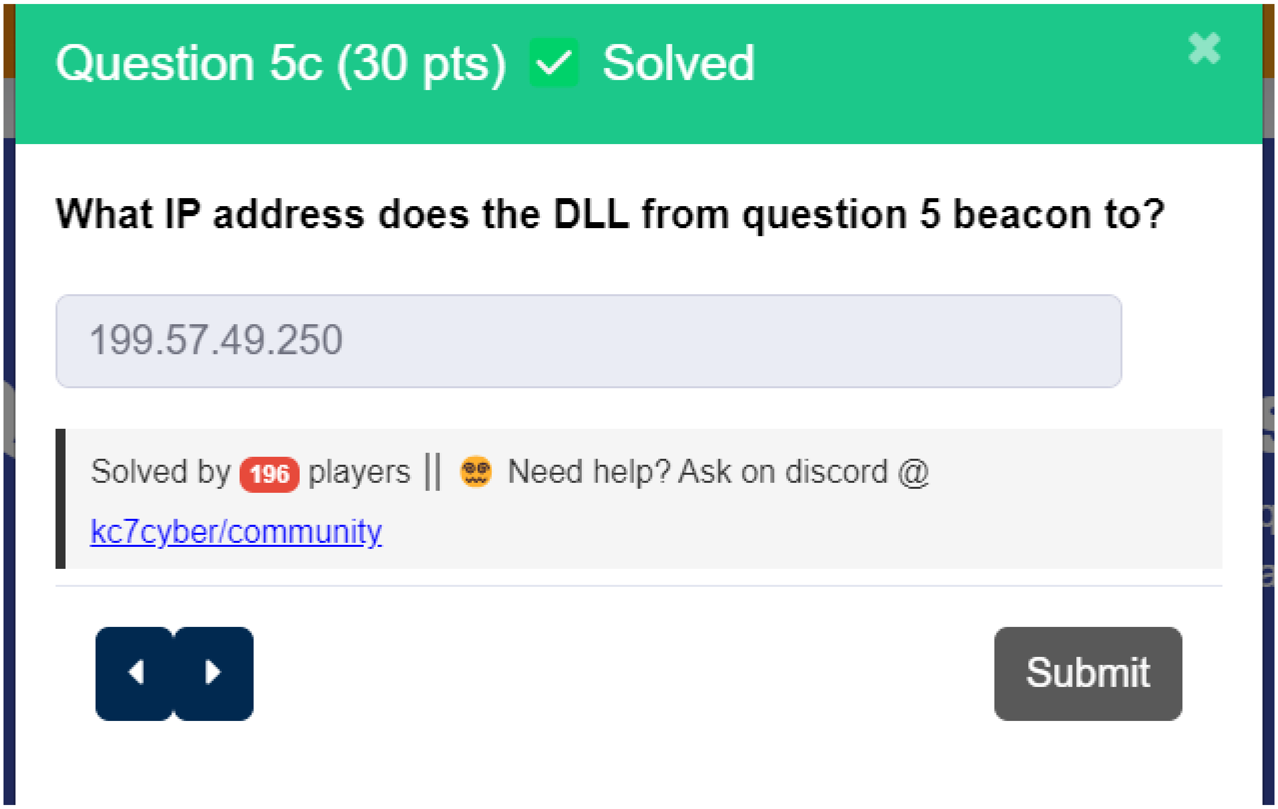
Solved by 201 players || Need help? Ask on discord @ kc7cyber/community



```
ProcessEvents
| where hostname == "DLY5-DESKTOP"
```

timestamp	parent_process_name	parent_process_hash	process_commandline	process_name	process_hash	hostname
2022-01-07 ...	updater.dll	1dc1dbfc1d636fed5ce...	whoami	cmd.exe	5fd13949d6a1f...	DLY5-DESKT...

```
"timestamp": 2022-01-07T14:03:35.328613Z,
"parent_process_name": updater.dll,
"parent_process_hash": 1dc1dbfc1d636fed5cebe43787a7abf2df4fbb51e1beaec34ba72dd5152edc81,
"process_commandline": whoami,
"process_name": cmd.exe,
"process_hash": 5fd13949d6a1f0ab9bc8a6424e63fdabe6f97b1587e47110a4ea5d56712786b3,
"hostname": DLY5-DESKTOP
```

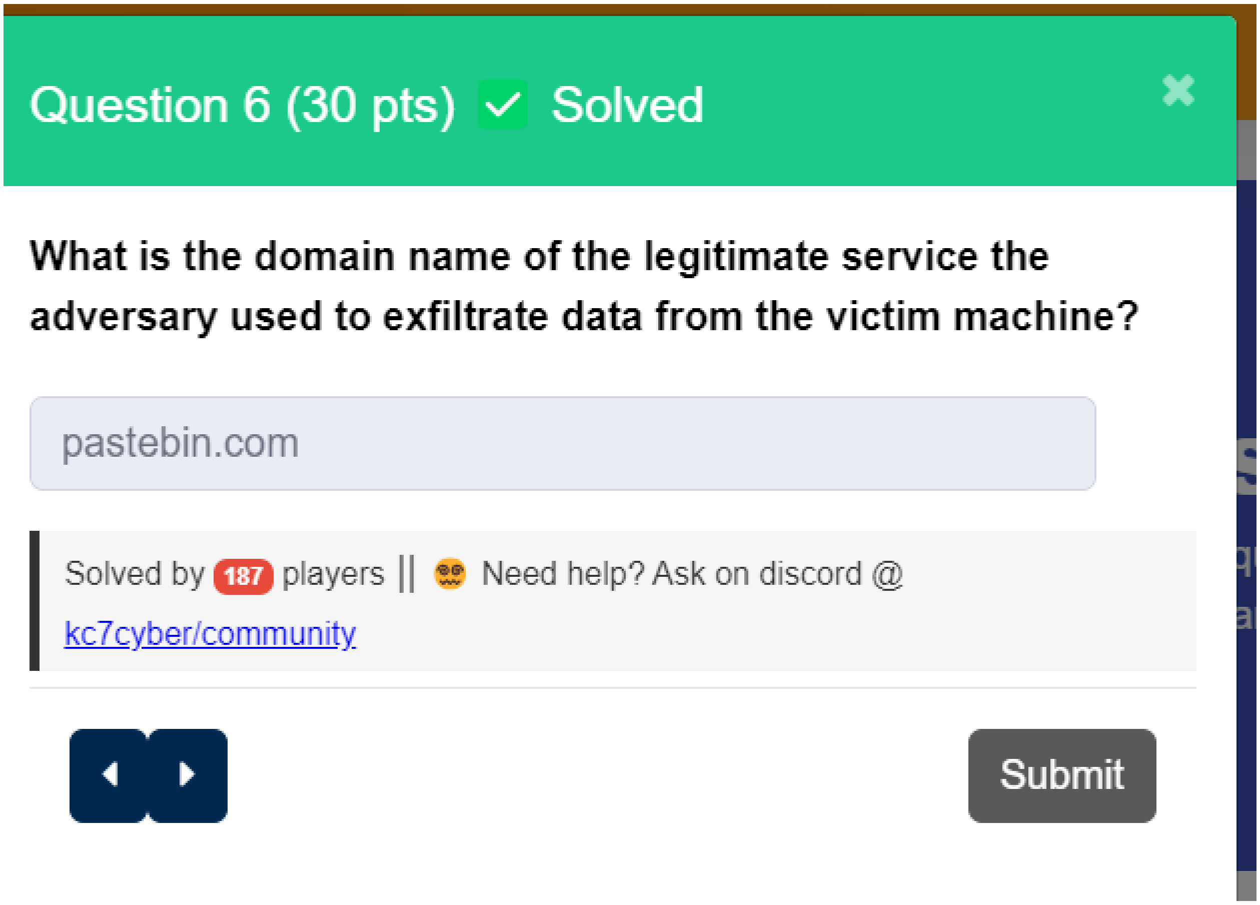


Question 5c (30 pts) ✓ Solved

What IP address does the DLL from question 5 beacon to?

199.57.49.250

Solved by 196 players || Need help? Ask on discord @ kc7cyber/community

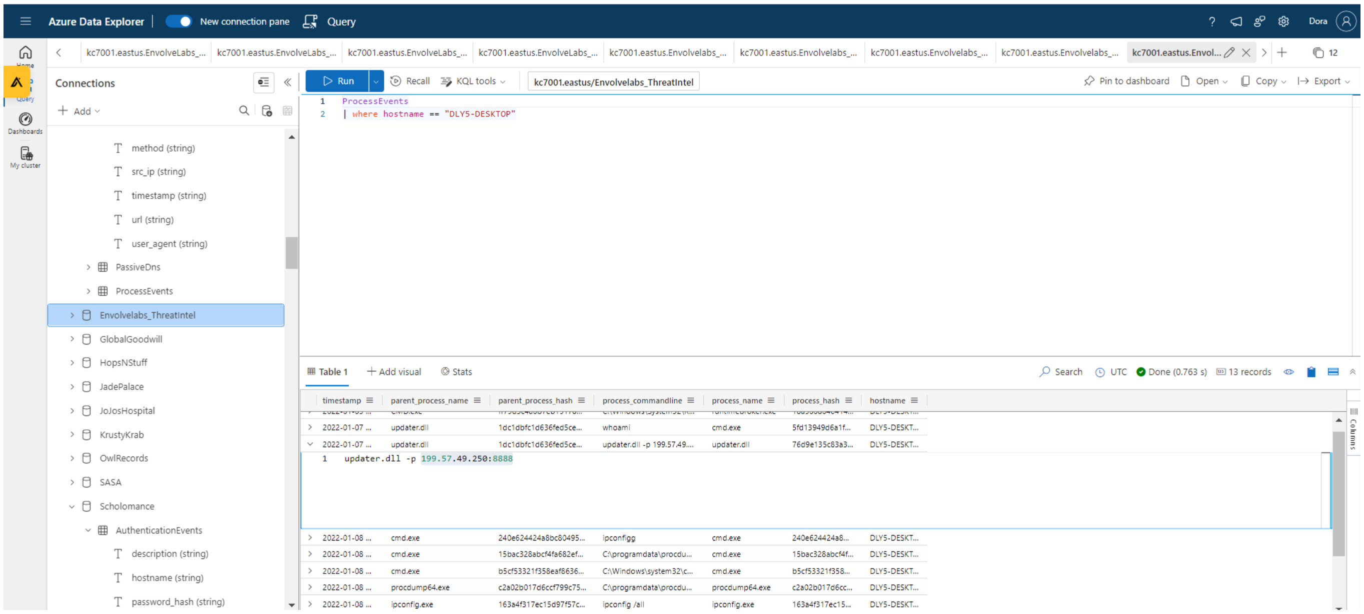


Question 6 (30 pts) ✓ Solved

What is the domain name of the legitimate service the adversary used to exfiltrate data from the victim machine?

pastebin.com

Solved by 187 players || Need help? Ask on discord @ kc7cyber/community



kc7001.eastus/Envolvelabs_ThreatIntel

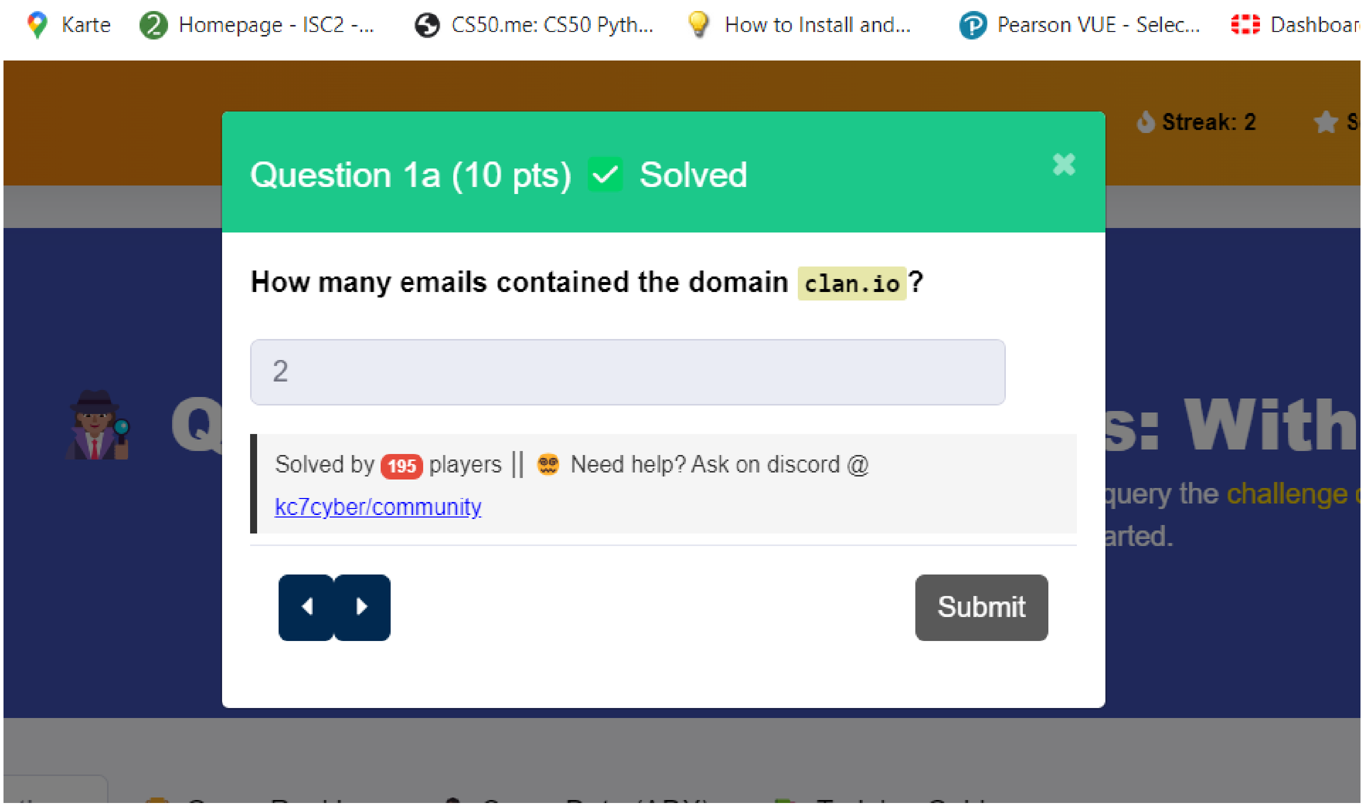
```
ProcessEvents
| where hostname == "DLY5-DESKTOP"
```

- method (string)
- src_ip (string)
- timestamp (string)
- url (string)
- user_agent (string)
- PassiveDns
- ProcessEvents
- Envolvelabs_ThreatIntel
- GlobalGoodwill
- HopsNStuff
- JadePalace
- JoJosHospital
- KrustyKrab
- OwlRecords
- SASA
- Scholomance
  - AuthenticationEvents
    - description (string)
    - hostname (string)
    - password_hash (string)

timestamp	parent_process_name	parent_process_hash	process_commandline	process_name	process_hash	hostname
2022-01-07 ...	updater.dll	1dc1dbfc1d636fed5ce...	whoami	cmd.exe	5fd13949d6a1f...	DLY5-DESKT...
2022-01-07 ...	updater.dll	1dc1dbfc1d636fed5ce...	updater.dll -p 199.57.49....	updater.dll	76d9e135c83a3...	DLY5-DESKT...

```
updater.dll -p 199.57.49.250:8888
```

timestamp	parent_process_name	parent_process_hash	process_commandline	process_name	process_hash	hostname
2022-01-08 ...	cmd.exe	240e624424a8bc80495...	ipconfigg	cmd.exe	240e624424a8...	DLY5-DESKT...
2022-01-08 ...	cmd.exe	15bac328abcf4fa682ef...	C:\programdata\procdu...	cmd.exe	15bac328abcf4f...	DLY5-DESKT...
2022-01-08 ...	cmd.exe	b5cf53321f358eaf8636...	C:\Windows\system32\c...	cmd.exe	b5cf53321f358...	DLY5-DESKT...
2022-01-08 ...	procdump64.exe	c2a02b017d6ccf799c75...	C:\programdata\procdu...	procdump64.exe	c2a02b017d6cc...	DLY5-DESKT...
2022-01-08 ...	ipconfig.exe	163a4f317ec15d97f57c...	ipconfig /all	ipconfig.exe	163a4f317ec15...	DLY5-DESKT...

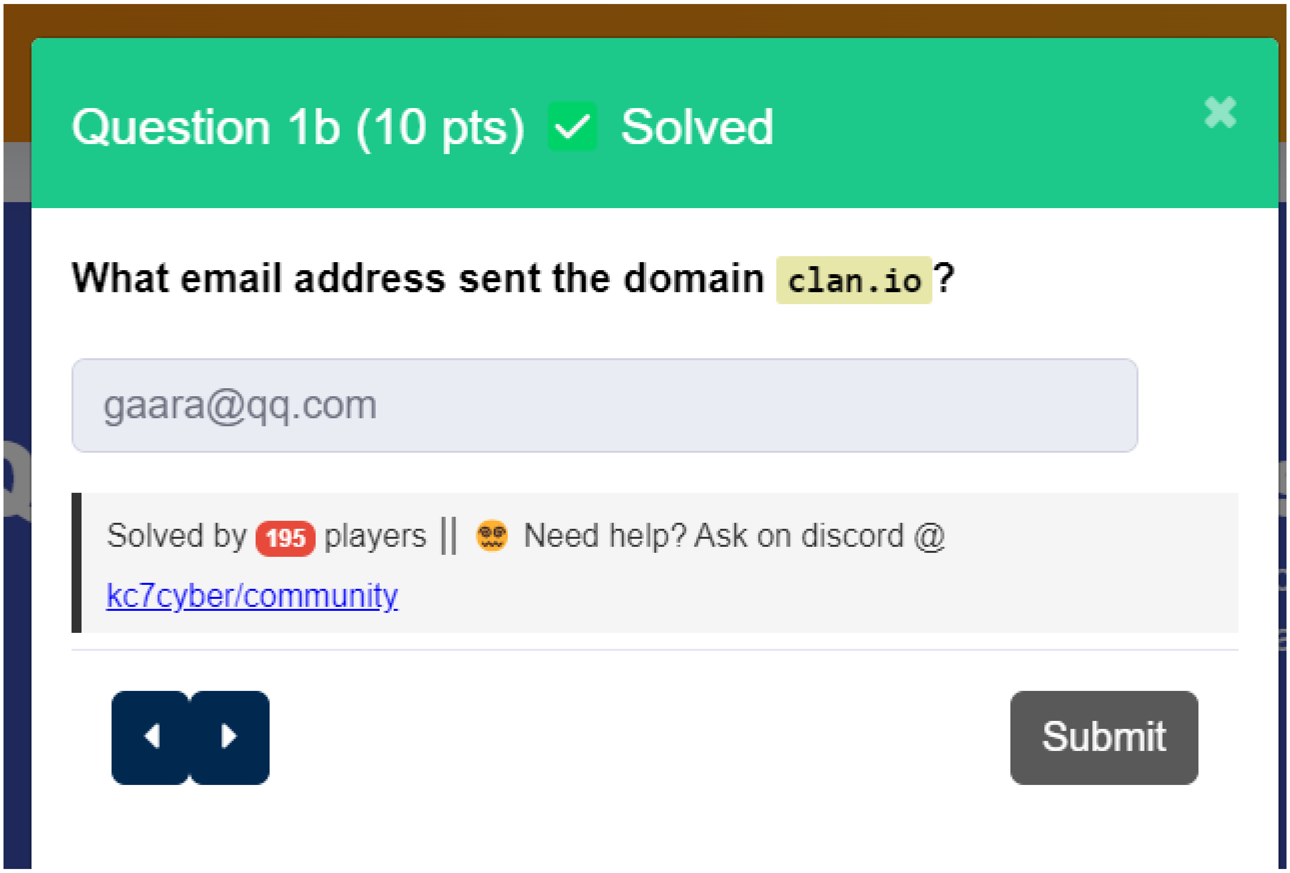


Question 1a (10 pts) ✓ Solved

How many emails contained the domain `clan.io`?

2

Solved by 195 players || Need help? Ask on discord @ kc7cyber/community

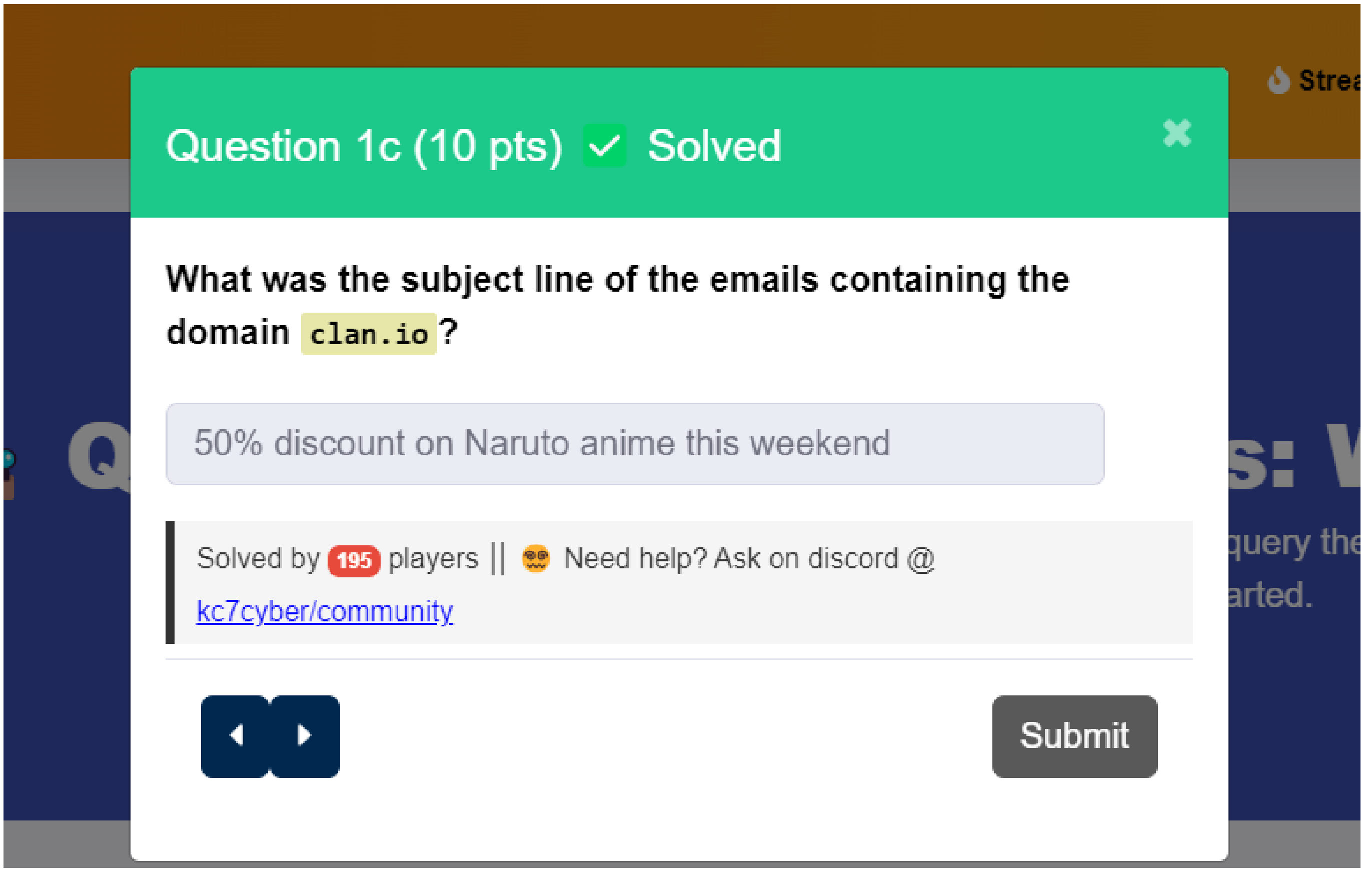


Question 1b (10 pts) ✓ Solved

What email address sent the domain `clan.io`?

gaara@qq.com

Solved by 195 players || Need help? Ask on discord @ kc7cyber/community

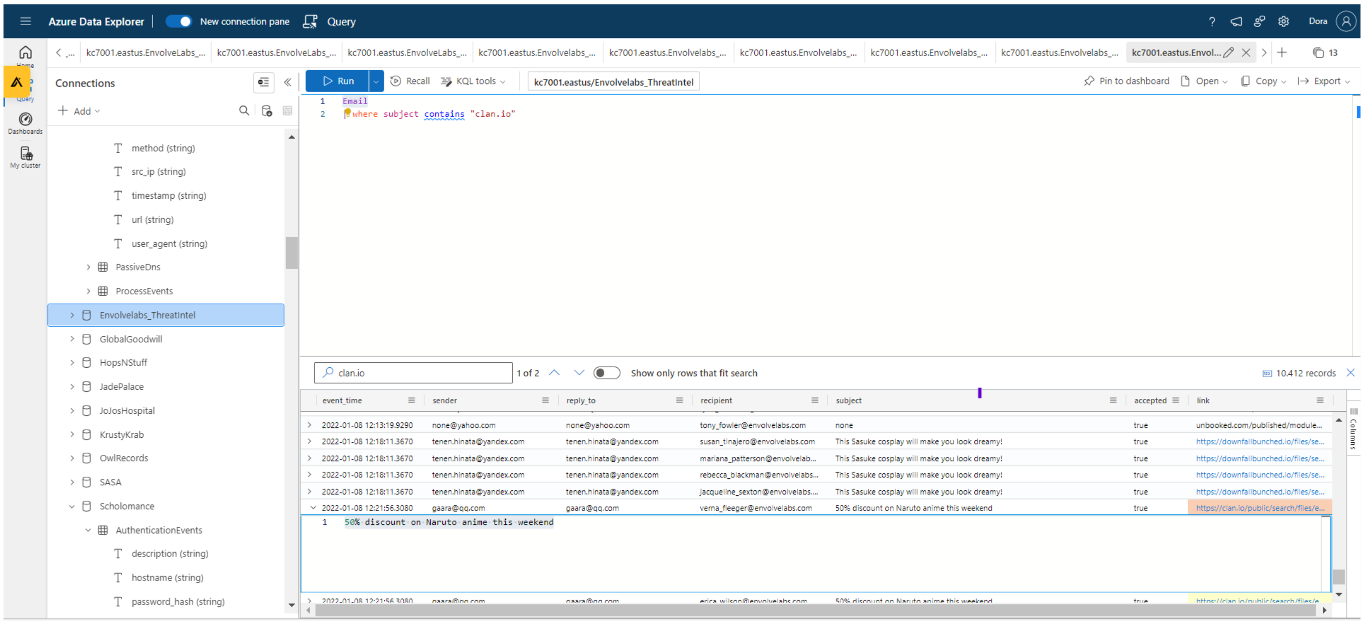


Question 1c (10 pts) ✓ Solved

What was the subject line of the emails containing the domain `clan.io`?

50% discount on Naruto anime this weekend

Solved by 195 players || Need help? Ask on discord @ kc7cyber/community



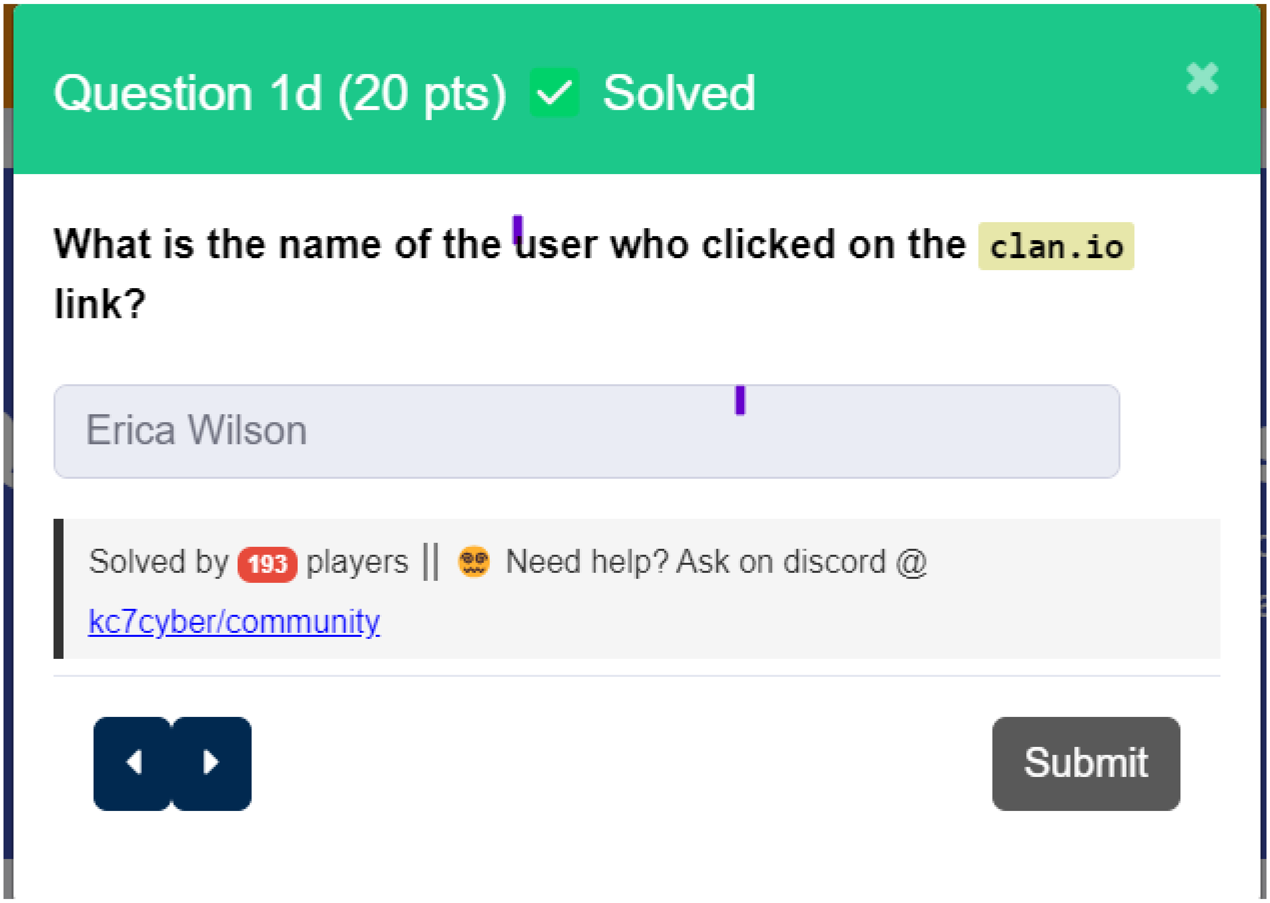
```
Email
| where subject contains "clan.io"
```

clan.io 1 of 2 Show only rows that fit search 10.412 records

event_time	sender	reply_to	recipient	subject	accepted	link
2022-01-08 12:13:19.9290	none@yahoo.com	none@yahoo.com	tony_fowler@envolvelabs.com	none	true	unbooked.com/published/module...
2022-01-08 12:18:11.3670	tenen.hinata@yandex.com	tenen.hinata@yandex.com	susan_tinajero@envolvelabs.com	This Sasuke cosplay will make you look dreamy!	true	https://downfallbunched.io/files/se...
2022-01-08 12:18:11.3670	tenen.hinata@yandex.com	tenen.hinata@yandex.com	mariana_patterson@envolvelab...	This Sasuke cosplay will make you look dreamy!	true	https://downfallbunched.io/files/se...
2022-01-08 12:18:11.3670	tenen.hinata@yandex.com	tenen.hinata@yandex.com	rebecca_blackman@envolvelabs...	This Sasuke cosplay will make you look dreamy!	true	https://downfallbunched.io/files/se...
2022-01-08 12:18:11.3670	tenen.hinata@yandex.com	tenen.hinata@yandex.com	jacqueline_sexton@envolvelabs....	This Sasuke cosplay will make you look dreamy!	true	https://downfallbunched.io/files/se...
2022-01-08 12:21:56.3080	gaara@qq.com	gaara@qq.com	verna_fleeger@envolvelabs.com	50% discount on Naruto anime this weekend	true	https://clan.io/public/search/files/e...

```
1   50% discount on Naruto anime this weekend
```

2022-01-08 12:21:56.3080	gaara@qq.com	gaara@qq.com	erica_wilson@envolvelabs.com	50% discount on Naruto anime this weekend	true	https://clan.io/public/search/files/e...

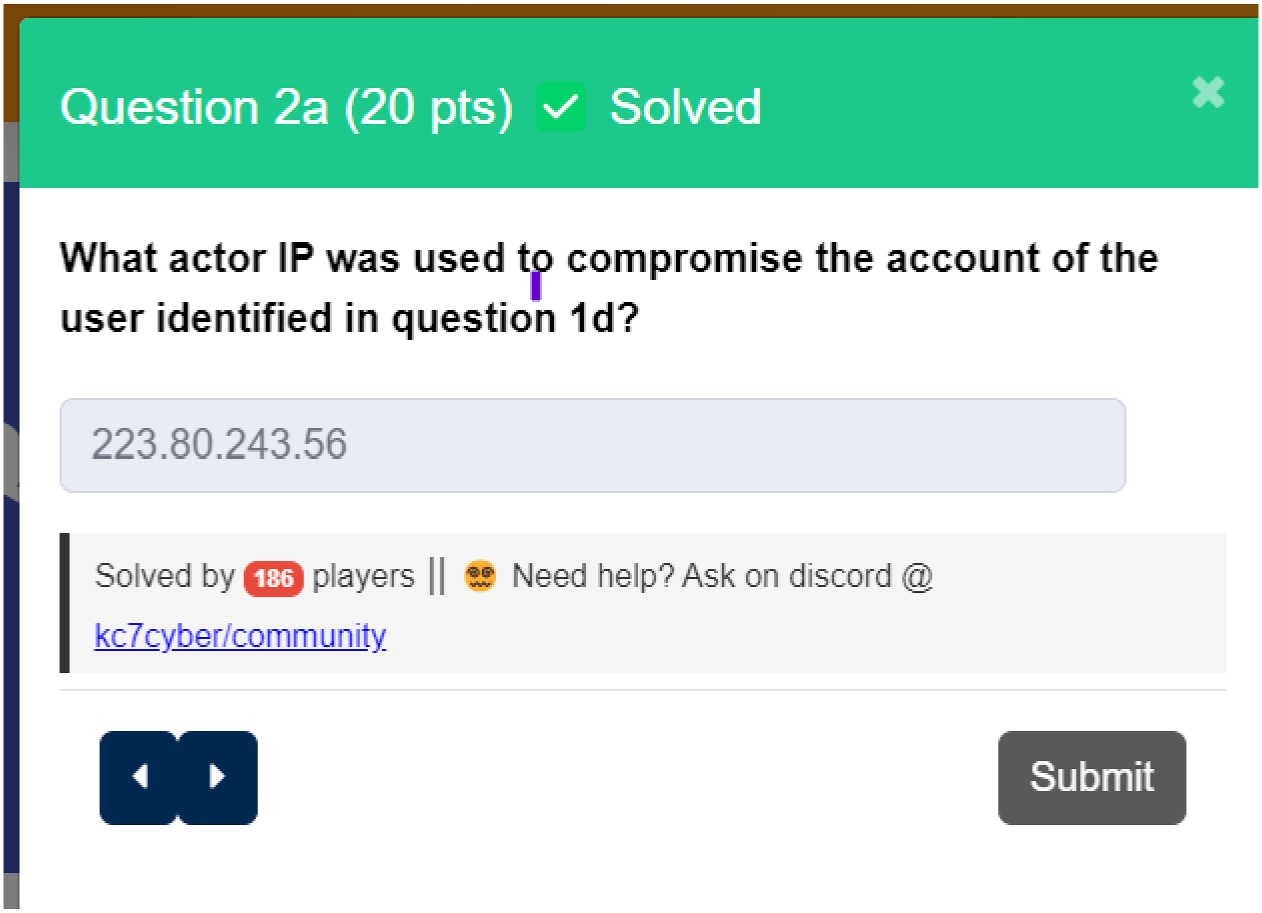


Question 1d (20 pts) ✓ Solved

What is the name of the user who clicked on the `clan.io` link?

Erica Wilson

Solved by 193 players || Need help? Ask on discord @ kc7cyber/community

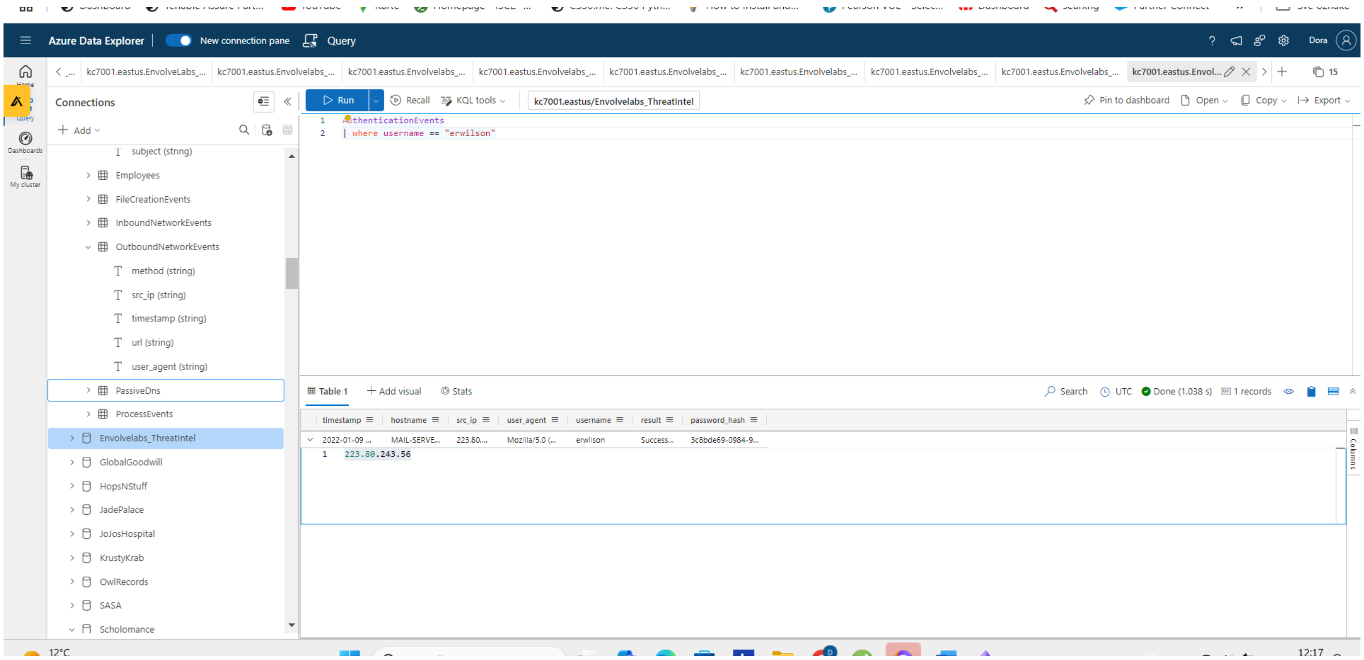


Question 2a (20 pts) ✓ Solved

What actor IP was used to compromise the account of the user identified in question 1d?

223.80.243.56

Solved by 186 players || Need help? Ask on discord @ kc7cyber/community



kc7001.eastus/Envolvelabs_ThreatIntel

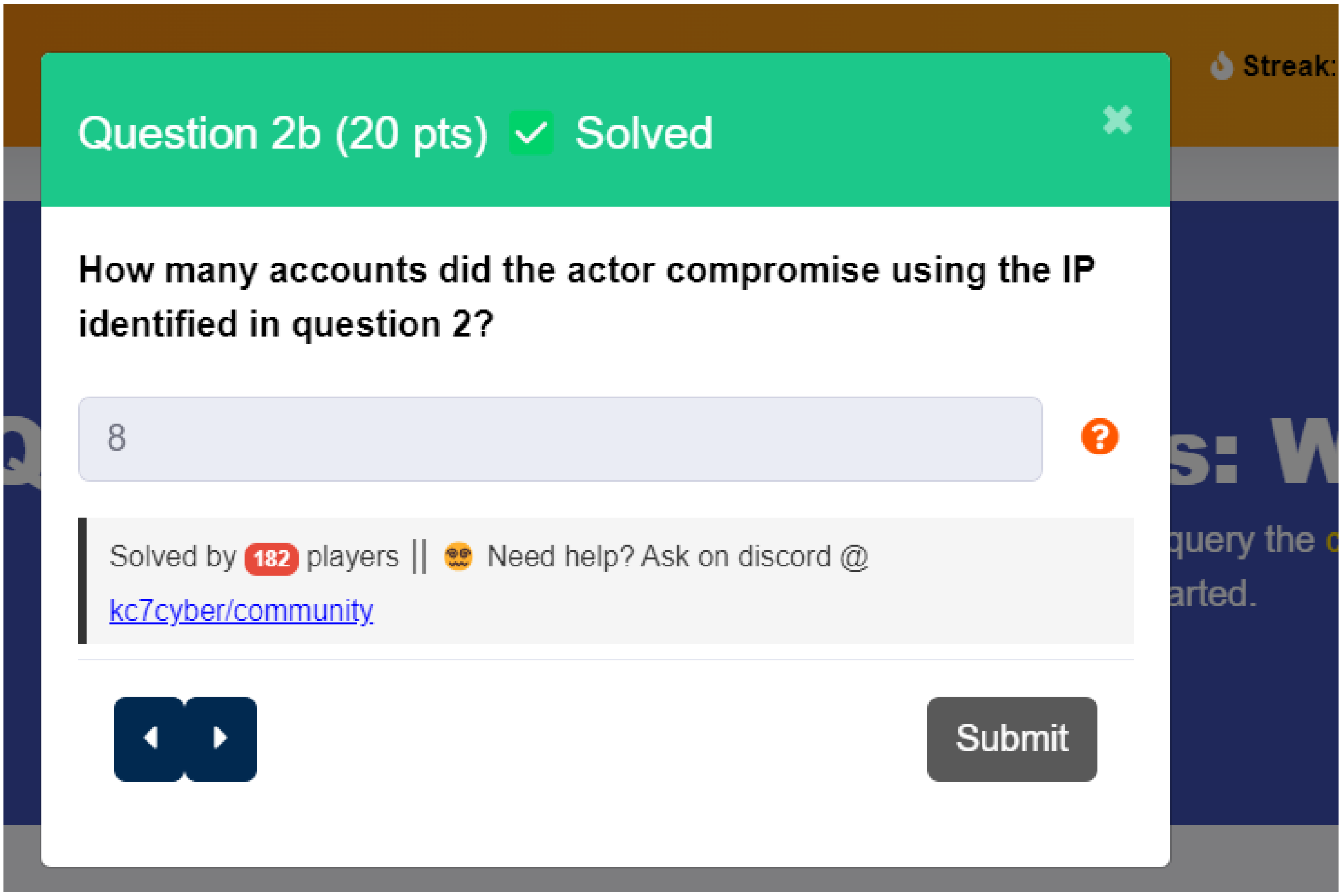
- subject (string)
- Employees
- FileCreationEvents
- InboundNetworkEvents
- OutboundNetworkEvents
  - method (string)
  - src_ip (string)
  - timestamp (string)
  - url (string)
  - user_agent (string)
- PassiveDns
- ProcessEvents
- Envolvelabs_ThreatIntel
- GlobalGoodwill
- HopsNStuff
- JadePalace
- JoJosHospital
- KrustyKrab
- OwlRecords
- SASA
- Scholomance

```
AuthenticationEvents
| where username == "erwilson"
```

Table 1 | Add visual | Stats — Done (1.038 s) 1 records

timestamp	hostname	src_ip	user_agent	username	result	password_hash
2022-01-09 ...	MAIL-SERVE...	223.80....	Mozilla/5.0 (...	erwilson	Success...	3c8bde69-0984-9...

```
1   223.80.243.56
```

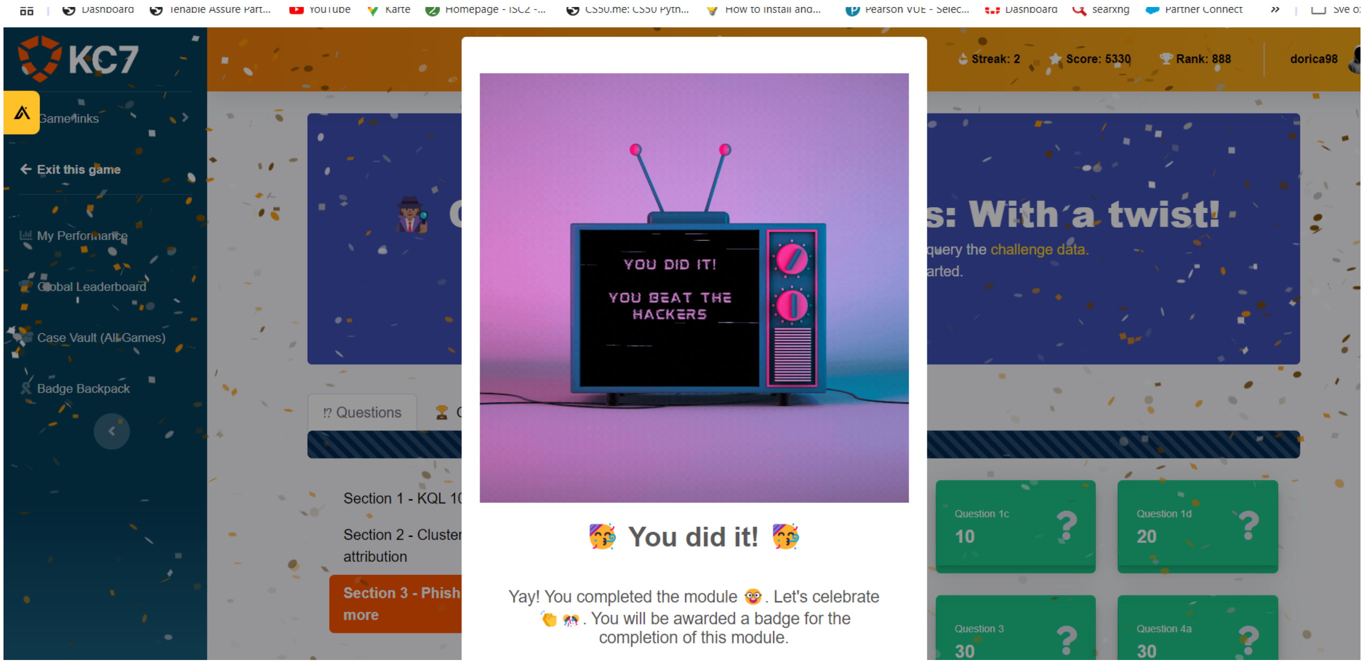


Question 2b (20 pts) ✓ Solved

How many accounts did the actor compromise using the IP identified in question 2?

8

Solved by 182 players || Need help? Ask on discord @ kc7cyber/community



🥳 You did it! 🥳

Yay! You completed the module 🤓. Let's celebrate 👏 🎊. You will be awarded a badge for the completion of this module.