Constellation

#sherlock #forensics #url-forensics #unfurl

Summary

Sherlock Category: Threat Intelligence
Release Date: 2023/12/14
Sherlock Creator: CyberJunkie
Summary: This was a really fun Sherlock that involved forensic analysis of two URLs. I wanted to share this because I guess I wasn't that aware of how much information can be obtained from more closely analyzing URLs. This Sherlock has you examine a Discord and Google Search URL and at the end of it, you'll have created a timeline for the events that transpired.

Table of Contents

Sherlock Scenario

> **Sherlock Scenario**
>
> The SOC team has recently been alerted to the potential existence of an insider threat. The suspect employee's workstation has been secured and examined. During the memory analysis, the Senior DFIR Analyst succeeded in extracting several intriguing URLs from the memory. These are now provided to you for further analysis to uncover any evidence, such as indications of data exfiltration or contact with malicious entities. Should you discover any information regarding the attacking group or individuals involved, you will collaborate closely with the threat intelligence team. Additionally, you will assist the Forensics team in creating a timeline. Warning : This Sherlock will require an element of OSINT and some answers can be found outside of the provided artifacts to complete fully.

Tasks

```
1) When did the suspect first start Direct Message (DM) conversations with the external entity (A possible threat actor group which targets organizations by paying employees to leak sensitive data)? (UTC)

2) What was the name of the file sent to the suspected insider threat?

3) When was the file sent to the suspected insider threat? (UTC)

4) The suspect utilized Google to search something after receiving the file. What was the search query?

5) The suspect originally typed something else in search tab, but found a Google search result suggestion which they clicked on. Can you confirm which words were written in search bar by the suspect originally?

6) When was this Google search made? (UTC)

7) What is the name of the Hacker group responsible for bribing the insider threat?

8) What is the name of the person suspected of being an Insider Threat?

9) What is the anomalous stated creation date of the file sent to the insider threat? (UTC)

10) The Forela threat intel team are working on uncovering this incident. Any OpSec mistakes made by the attackers are crucial for Forela's security team. Try to help the TI team and confirm the real name of the agent/handler from Anticorp.

11) Which City does the threat actor belong to?
```

Artifacts

After downloading the `constellation.zip` from the HTB website and unzipping, we're left with two files to examine.

```
unzip constellation.zip
Archive:  constellation.zip
   creating: Artifacts/
[constellation.zip] Artifacts/IOCs.txt password:

tree .
.
├── Artifacts
│   ├── IOCs.txt
│   └── NDA_Instructions.pdf

1 directory, 2 files
```

IOCs.txt

```
URL 1 :
https://cdn.discordapp.com/attachments/1152635915429232640/1156461980652154931/NDA_Inst
ructions.pdf?
ex=65150ea6&is=6513bd26&hm=64de12da031e6e91cc4f35c64b2b0190fb040b69648a64365f8a82607606
56e3&

URL 2 : https://www.google.com/search?
q=how+to+zip+a+folder+using+tar+in+linux&sca_esv=568736477&hl=en&sxsrf=AM9HkKkFWLlX_hC6
3KqDpJwdH9M3JL7LZA%3A1695792705892&source=hp&ei=Qb4TZeL2M9XPxc8PwLa52Ag&iflsig=AO6bgOgA
AAAAZRPMUXuGExueXDMxHxU9iRXOL-GQIJZ-
&oq=How+to+archive+a+folder+using+tar+i&gs_lp=Egdnd3Mtd2l6IiNIb3cgdG8gYXJjaGl2ZSBhIGZvb
GRlciB1c2luZyB0YXIgaSoCCAAyBhAAGBYYHjIIEAAYigUYhgMyCBAAGIoFGIYDMggQABiKBRiGA0jI3QJQ8WlY
xIUCcAx4AJABAJgBqQKgAeRWqgEEMi00NrgBAcgBAPgBAagCCsICBxAjGOoCGCfCAgcQIxiKBRgnwgIIEAAYigU
YkQLCAgsQABiABBixAxiDAcICCBAAGIAEGLEDwgILEAAYigUYsQMYgwHCAggQABiKBRixA8ICBBAjGCfCAgcQAB
iKBRhDwgIOEC4YigUYxwEY0QMYkQLCAgUQABiABMICDhAAGIoFGLEDGIMBGJECwgIFEC4YgATCAgoQABiABBgUG
IcCwgIFECEYoAHCAgUQABiiBMICBxAhGKABGArCAggQABgWGB4YCg&sclient=gws-wiz
```

We're given two URLs, one being what appears to be a Discord download and the other being a Google Search.

NDA_Instructions.pdf

This is a PDF from `AntiCorp Gr04p`, that walks an individual, `karen riley`, through compressing a file with `tar` and then uploading it to an S3 bucket, `s3://hahaha-you-lose-forela/` with the AWS CLI. It also promises `$20,000`, which will be sent to their PayPal account.

OSINT

The Sherlock Scenario mentions some OSINT work will be needed, so the first thing I did was search for `"AntiCorp Gr04p"`. The first result is for a LinkedIn profile - https://pk.linkedin.com/in/abdullah-al-sajjad-434545293. The individual, `Abdullah Al Sajjad`, is a "Security Expert at AntiCorp Gr04p" and is from "Bahawalpur, Punjab, Pakistan".

Abdullah also has the following post on their profile:

```
I need people who are proficient in developing fud  deliverables like macro docs, pdfs
and other stuff . These are for Confidential Red team engagements. Email me on
CyberJunkie@AntiCorp.Gr04p
```

There are no comments or anything else to lead us to when `karen riley`, might've reached out to this group. I tried doing some more OSINT on `Abdullah Al Sajjad`, `karen riley`, `AntiCorp Gr04p`, and `@AntiCorp.Gr04p`, but yielded no results.

File Metadata

With OSINT giving us nothing else to work off of, I went back to the `NDA_Instructions.pdf` (which we know comes from hacking group).

```
exiftool NDA_Instructions.pdf
ExifTool Version Number         : 12.76
File Name                       : NDA_Instructions.pdf
Directory                       : .
File Size                       : 26 kB
File Modification Date/Time     : 2024:03:05 05:02:19-05:00
File Access Date/Time           : 2024:07:24 20:41:33-04:00
File Inode Change Date/Time     : 2024:07:24 20:40:10-04:00
File Permissions                : -rw-rw-r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.7
Linearized                      : No
Page Count                      : 1
Producer                        : AntiCorp PDF FW
Create Date                     : 2054:01:17 22:45:22+01:00
Title                           : KarenForela_Instructions
Author                          : CyberJunkie@AntiCorp.Gr04p
Creator                         : AntiCorp
Modify Date                     : 2054:01:17 22:45:22+01:00
```

```
Subject                          : Forela_Mining stats and data campaign (Stop
destroying env)
```

One interesting piece of information is that the file was supposedly created `2054-01-17 22:45:22`.

I also initially found `CyberJunkie@AntiCorp.Gr04p` interesting, until I learned `CyberJunkie` is just the creator of the Sherlock and OSINT there yielded no results.

Given [Task 10], `Forela` is the name of the company that `karen riley` works for. I tried doing some OSINT on `Forela Mining` & `Forela`, but that yielded no promising results either.

URL Forensics

All that is left are the two URLs within `IOCs.txt`

```
URL 1 :
https://cdn.discordapp.com/attachments/1152635915429232640/1156461980652154931/NDA_Inst
ructions.pdf?
ex=65150ea6&is=6513bd26&hm=64de12da031e6e91cc4f35c64b2b0190fb040b69648a64365f8a82607606
56e3&

URL 2 : https://www.google.com/search?
q=how+to+zip+a+folder+using+tar+in+linux&sca_esv=568736477&hl=en&sxsrf=AM9HkKkFWLlX_hC6
3KqDpJwdH9M3JL7LZA%3A1695792705892&source=hp&ei=Qb4TZeL2M9XPxc8PwLa52Ag&iflsig=AO6bgOgA
AAAAZRPMUXuGExueXDMxHxU9iRXOL-GQIJZ-
&oq=How+to+archive+a+folder+using+tar+i&gs_lp=Egdnd3Mtd2l6IiNIb3cgdG8gYXJjaGl2ZSBhIGZvb
GRlciB1c2luZyB0YXIgaSoCCAAyBhAAGBYYHjIIEAAYigUYhgMyCBAAGIoFGIYDMggQABiKBRiGA0jI3QJQ8WlY
xIUCcAx4AJABAJgBqQKgAeRWqgEEMi00NrgBAcgBAPgBAagCCsICBxAjGOoCGCfCAgcQIxiKBRgnwgIIEAAYigU
YkQLCAgsQABiABBixAxiDAcICCBAAGIAEGLEDwgILEAAYigUYsQMYgwHCAggQABiKBRixA8ICBBAjGCfCAgcQAB
iKBRhDwgIOEC4YigUYxwEY0QMYkQLCAgUQABiABMICDhAAGIoFGLEDGIMBGJECwgIFEC4YgATCAgoQABiABBgUG
IcCwgIFECEYoAHCAgUQABiiBMICBxAhGKABGArCAggQABgWGB4YCg&sclient=gws-wiz
```

I searched for "URL forensics" and one of the first results was this blog post, a tool called `unfurl` (which I've never heard of). This tool takes a URL and graphs out the different components that make it up. As I mentioned in the summary, I wasn't aware of this and how much a URL can actually leak.

There are three ways to run `unfurl`:

1. In you browser - https://dfir.blog/unfurl/.
2. Via the command line interface.
3. Running the web app locally.

Setting up Unfurl

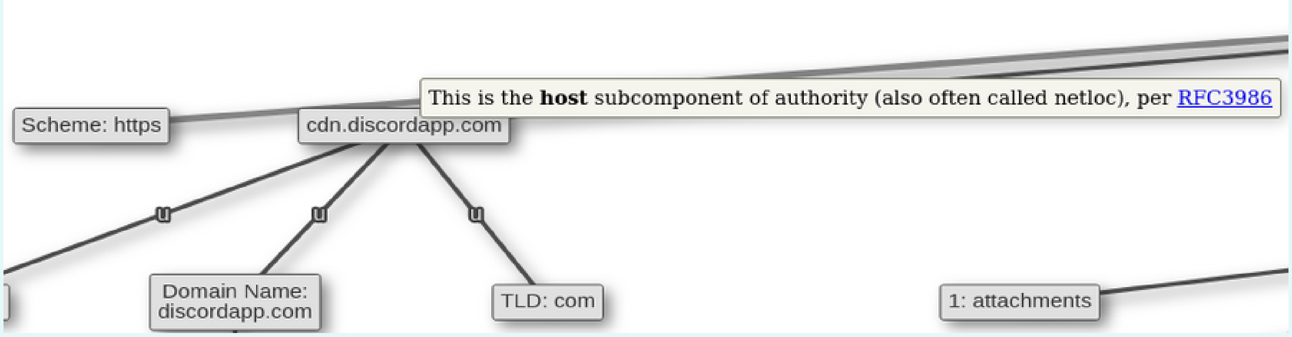
Running the web app locally:

```
git clone https://github.com/obsidianforensics/unfurl
cd unfurl
pip3 install -r requirements-all.txt
python3 unfurl/scripts/unfurl_app.py
```

After running `python3 unfurl/scripts/unfurl_app.py`, visit `http://localhost:5000` in your browser.

Fun Tip

When working with `unfurl`, if you hover over an item within the graph, it will explain what it is and how it derived it from the URL you entered.


This is the **host** subcomponent of authority (also often called netloc), per RFC3986
Scheme: https
cdn.discordapp.com
u
u
u
Domain Name: discordapp.com
TLD: com
1: attachments

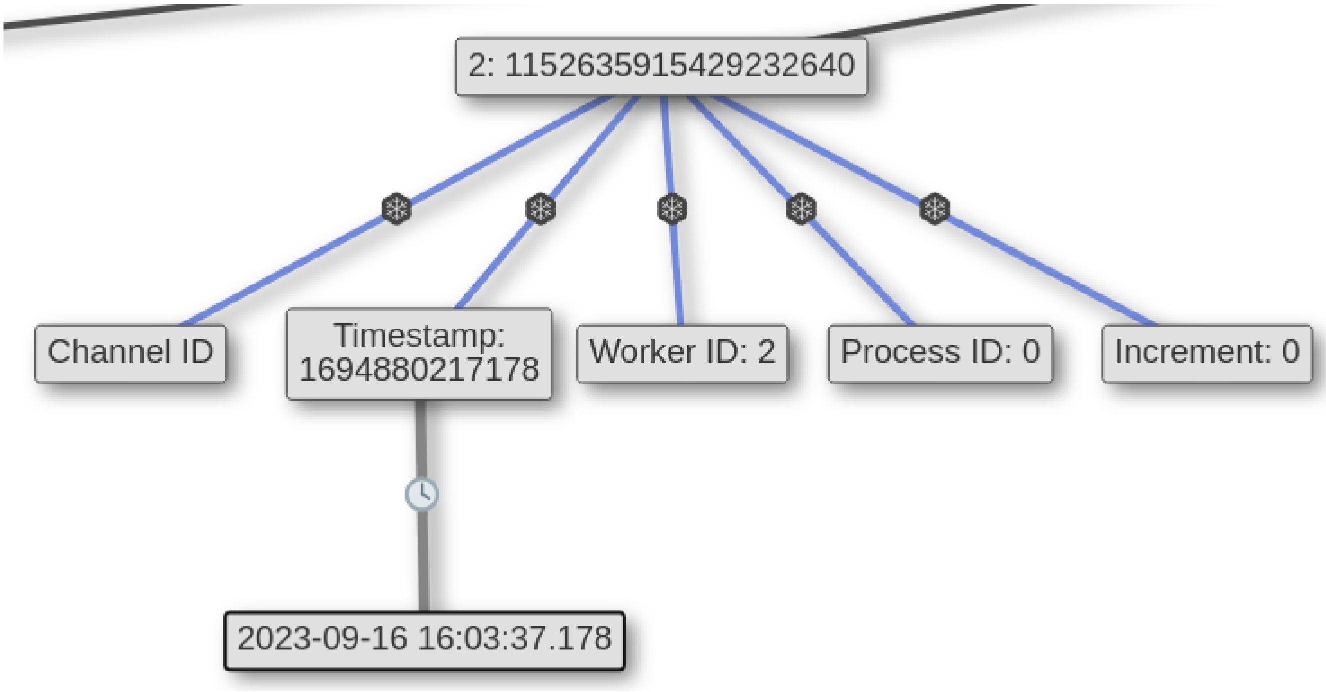
URL One (Discord)

You'll notice when entering the Discord URL the graph is presented breaking down what each part of it means.

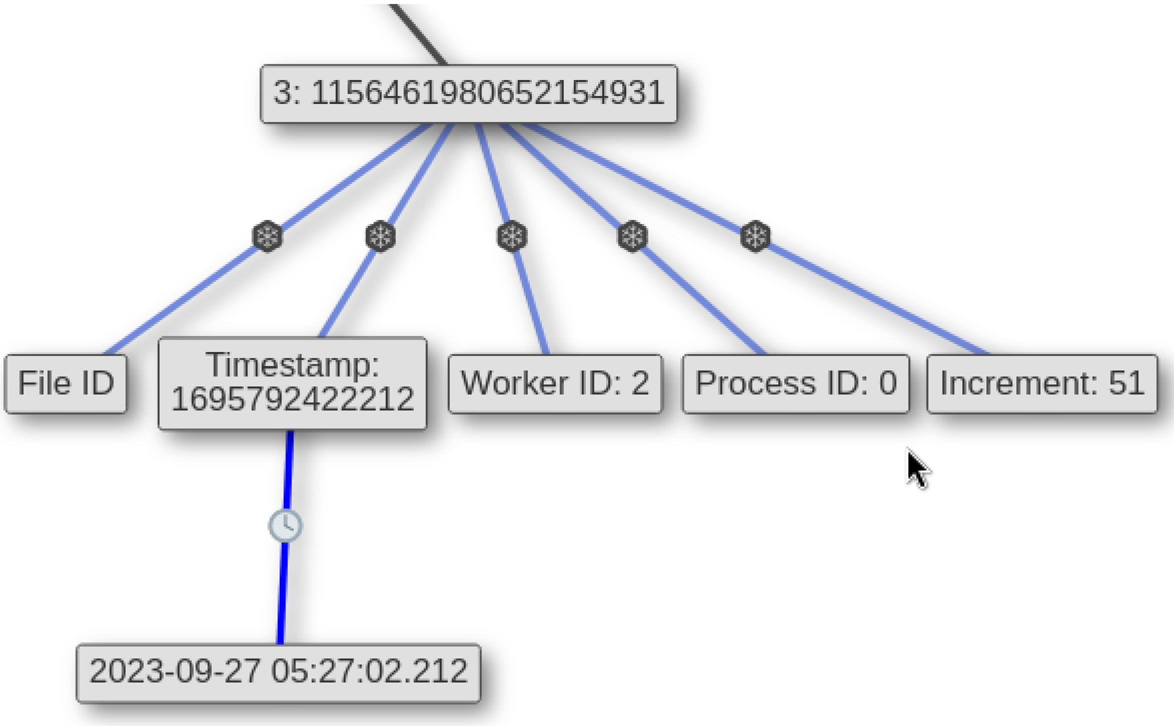
The `/attachments/1152635915429232640/1156461980652154931/NDA_Instructions.pdf` section is broken into four parts.

1. `attachments` - which I'm not too sure what this is besides telling us it's a Discord download.
2. `Channel ID` - when the DM between the hacking group & the insider threat was created.
3. `File ID` - information about when the file was sent.
4. `NDA_Instructions.pdf` - shows the file name and file extension.

Channel ID



File ID



Discord Analysis

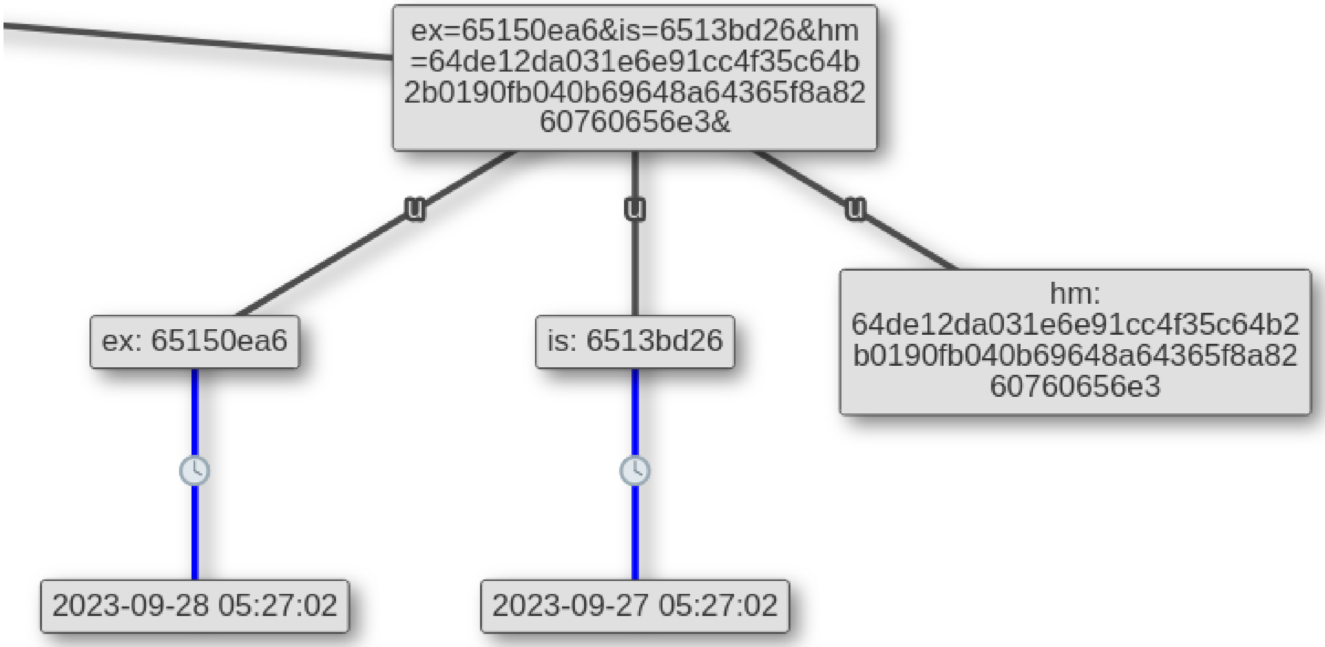
Based on the images above we now know the following:

1. Discord was used between the hacking group (`Abdullah Al Sajjad`) and the insider threat (`karen riley`).

2. Their conversations started on `2023-09-16 16:03:37 UTC`.
3. The `NDA_Instructions.pdf` was sent on `2023-09-27 05:27:02 UTC` (roughly 11 days later).

(Optional Read) More on Discord Parameters

This section is optional and has nothing to do with the Sherlock. Since this is all so new to me, I was curious what the other data meant. When researching these parameters I came across this BleepingComputer article. Discord implemented these to block malware delivery on their service (or at least make it harder).


ex=65150ea6&is=6513bd26&hm=64de12da031e6e91cc4f35c64b2b0190fb040b69648a64365f8a8260760656e3&
u
u
u
ex: 65150ea6
is: 6513bd26
hm: 64de12da031e6e91cc4f35c64b2b0190fb040b69648a64365f8a8260760656e3
2023-09-28 05:27:02
2023-09-27 05:27:02

`hm` is a signature. I'm assuming it's like an ID that the Discord team can look back at when files are flagged (or potentially the signature is used to flag suspicious/malicious files.)

`ex` is the expiration timestamp (when it'll be removed from Discord servers). According to Discord, this is a 24 hour period.

The article doesn't go into what `is` actually is. Based on the timestamp being 24 hours apart from `ex` (the expiration timestamp) and matching the `File ID` timestamp (which we know from earlier was when the file was sent), `is` must be the timestamp when the file was sent/created. It is also entirely possible, the timestamp under `File ID` is grabbed from this `is` parameter.

URL Two (Google Search)

The `unfurl` for the Google Search URL is a lot bigger and more complex. Due to that, I'm only going to show the important bits so everything can be seen clearly.

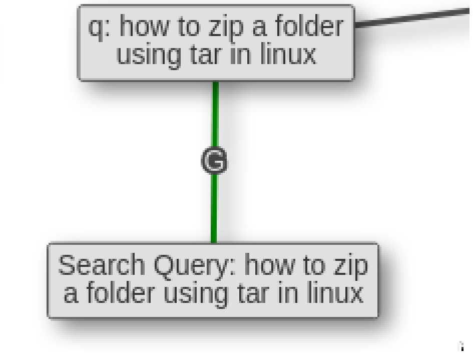
URL 2

I attempted to breakdown the URL below by parameter so it'd be easier to see what this link is hiding.

```
https://www.google.com/search
?q=how+to+zip+a+folder+using+tar+in+linux
&sca_esv=568736477
&hl=en
&sxsrf=AM9HkKkFWLlX_hC63KqDpJwdH9M3JL7LZA%3A1695792705892
&source=hp
&ei=Qb4TZeL2M9XPxc8PwLa52Ag
&iflsig=AO6bgOgAAAAAZRPMUXuGExueXDMxHxU9iRXOL-GQIJZ-
&oq=How+to+archive+a+folder+using+tar+i
&gs_lp=Egdnd3Mtd2l6IiNIb3cgdG8gYXJjaGl2ZSBhIGZvbGRlciB1c2luZyB0YXIgaSoCCAAyBhAAGBYYHjII
EAAYigUYhgMyCBAAGIoFGIYDMggQABiKBRiGA0jI3QJQ8WlYxIUCcAx4AJABAJgBqQKgAeRWqgEEMi00NrgBAcg
BAPgBAagCCsICBxAjGOoCGCfCAgcQIxiKBRgnwgIIEAAYigUYkQLCAgsQABiABBixAxiDAcICCBAAGIAEGLEDwg
ILEAAYigUYsQMYgwHCAggQABiKBRixA8ICBBAjGCfCAgcQABiKBRhDwgIOEC4YigUYxwEY0QMYkQLCAgUQABiAB
MICDhAAGIoFGLEDGIMBGJECwgIFEC4YgATCAgoQABiABBgUGIcCwgIFECEYoAHCAgUQABiiBMICBxAhGKABGArC
AggQABgWGB4YCg&sclient=gws-wiz
```

Search Query

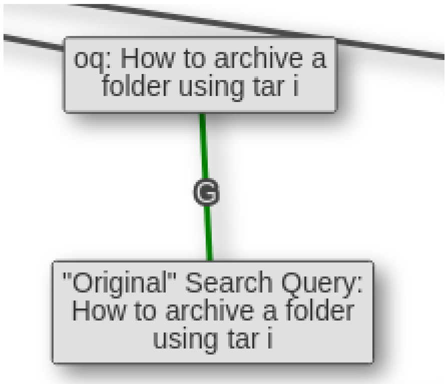
The query (the search that was made), can be seen with the `q=` parameter (`q=how+to+zip+a+folder+using+tar+in+linux`) - `how to zip a folder using tar in linux`.


q: how to zip a folder using tar in linux
G
Search Query: how to zip a folder using tar in linux

Original Query

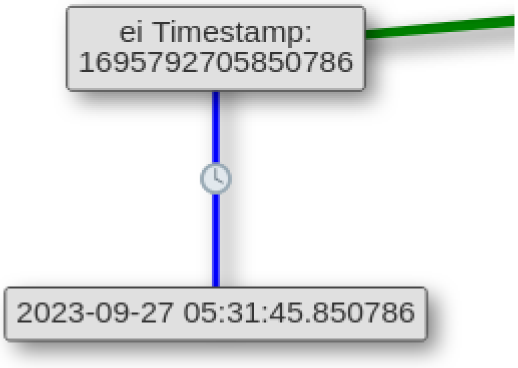
The original query can also be seen with the `oq` parameter (`&oq=How+to+archive+a+folder+using+tar+i`) - `How to archive a folder using tar i`.

This is what `karen riley` was typing, but Google suggested `how to zip a folder using tar in linux` and they clicked on that instead.


oq: How to archive a folder using tar i
"Original" Search Query: How to archive a folder using tar i

Timestamp

The timestamp when the Google Search was made is also visible with the `ei=` parameter (`ei=Qb4TZeL2M9XPxc8PwLa52Ag`). From `unfurl`: "The first two values combined in the `ei` parameter are thought to be the timestamp of when the session began. The first, `ei-0`, contains the full seconds portion of the timestamp and the second, `ei-1`, contains the fractional seconds."



The End

Putting it all together now:

```
1) When did the suspect first start Direct Message (DM) conversations with the external
entity (A possible threat actor group which targets organizations by paying employees
to leak sensitive data)? (UTC)

Answer: 2023-09-16 16:03:37 UTC
Source: Looking at the Channel ID timestamp (unfurl Discord URL).

2) What was the name of the file sent to the suspected insider threat?

Answer: NDA_Instructions.pdf
Source: We received this as part of the resources for this Sherlock.

3) When was the file sent to the suspected insider threat? (UTC)
```

```
Answer: 2023-09-27 05:27:02 UTC
Source: Looking at the File ID timestamp (unfurl Discord URL).

4) The suspect utilized Google to search something after receiving the file. What was
the search query?

Answer: how to zip a folder using tar in linux
Source: Analyazing the `q` parameter within the Google Search URL.

5) The suspect originally typed something else in search tab, but found a Google search
result suggestion which they clicked on. Can you confirm which words were written in
search bar by the suspect originally?

Answer: How to archive a folder using tar i
Source: Analyazing the `oq` parameter within the Google Search URL.

6) When was this Google search made? (UTC)

Answer: 2023-09-27 05:31:45
Source: Using `unfurl` revealed the timestamp.

7) What is the name of the Hacker group responsible for bribing the insider threat?

Answer: AntiCorp Gr04p
Source: Mentioned in the NDA_Instructions.pdf and on the LinkedIn page.

8) What is the name of the person suspected of being an Insider Threat?

Answer: Karen Riley
Source: Mentioned in the NDA_Instructions.pdf as well as the metadata.

9) What is the anomalous stated creation date of the file sent to the insider threat?
(UTC)

Answer: 2054-01-17 22:45:22
Source: Found in the metadata of NDA_Instructions.pdf.

10) The Forela threat intel team are working on uncovering this incident. Any OpSec
mistakes made by the attackers are crucial for Forela's security team. Try to help the
TI team and confirm the real name of the agent/handler from Anticorp.

Answer: Abdullah Al Sajjad
Source: OSINT on the group "AntiCorp Gr04p" revealed their LinkedIn page.

11) Which City does the threat actor belong to?
```

```
Answer: OSINT on the group "AntiCorp Gr04p" revealed their LinkedIn page.
Source: Bahawalpur
```

Links

HTB Profile: https://app.hackthebox.com/profile/160154
HTB Academy Referral Link: https://referral.hackthebox.com/mzw0ItT
Twitter / X: https://x.com/0xsaboten