



## Forensic Investigation of Instant Messaging Services on Linux OS: Discord and Slack as Case Studies

By:

Megan Davis (Virginia Commonwealth University), Bridget McInnes (Virginia Commonwealth University), and Irfan Ahmed (Virginia Commonwealth University)

*From the proceedings of*

The Digital Forensic Research Conference

**DFRWS USA 2022**

July 11-14, 2022

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment.

As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

**<https://dfrws.org>**

# Forensic Investigation of Instant Messaging Services on Linux OS: Discord and Slack as Case Studies



**Megan Davis**, Bridget McInnes, Irfan Ahmed  
Department of Computer Science  
Virginia Commonwealth University





## Table of Contents

1. Introduction
2. Methodology
3. Discord Results
4. Slack Results
5. Summary
6. Future Work



---

1

# Introduction





## Introduction

- Instant Messaging Applications (IMAs) saw wider adoption
  - Ex. Discord / Slack
- 2019 COVID
  - Shift from in-office to work from home model
  - Nearly 71% of employees went to WFH





## Discord

- Videogames, mostly associated with Twitch
- Electron Framework
- 140 million active users
- 2021 Discord removed thousands of servers
  - child harm material, cybercrime, doxxing, exploitative content, and extremist or violent content





# Discord

**Bio Studies**

# **study-questions**

**moongirl** Today at 9:18 AM  
\ ( ; ∇ ; ) / help. how is the answer not A?  
Light reactions photophosphorylate ADP, while the Calvin cycle produces ATP  
@everyone i thought this was right. can anyone clarify this for me?

**Josh** Today at 9:18 AM  
uhhh i also got A...LOL

**Katelin** Today at 9:18 AM  
me too...

**Josh** Today at 9:18 AM  
oh no i'm going to fail for sure

**Katelin** Today at 9:18 AM  
we got this

→ **jesu showed up!** Yesterday at 2:38PM

**Shawn** Today at 9:18 AM  
anyone wanna study together in voice?  
👤 3 🗣️ 3

**moongirl** Today at 9:18 AM  
this video really helped me!! give it a watch, it explains it pretty clearly  
<https://youtu.be/OIDx6aQ928o>

**MODERATORS — 4**

- Allan
- fiona
- Daniel
- moongirl  
Listening to Spotify

**MOLECULAR BIO — 5**

- Katelin
- terra
- James
- Sidequick  
Playing League of Legends
- Shawn

**ECOLOGY — 6**

- Serena  
Listening to Spotify
- gnarf
- Josh
- Amo  
Streaming Drawing 's-r-7
- muffins





## Slack

- Traditional Business
- Electron Framework
- Competitor to Microsoft Teams
- 2019, reported 12 million slack users
- Banned 27 accounts tied to hate groups







# Slack

The screenshot displays the Slack desktop application interface. On the left is a purple sidebar with navigation options: 'All unread', 'Threads', 'Mentions & reactions', 'Drafts', and 'Channels'. The 'Channels' section is expanded to show '# announcements', '# design-crit', '# media-and-pr', and the selected channel '# social-media'. Below channels are 'Direct messages' including 'slackbot', 'Zoe Maxwell (you)', and 'Lee Hao, Sara Parras'. The main workspace shows the '#social-media' channel with 21 members. Recent messages include an announcement for a 'Team Status Meeting' starting in 15 minutes, a note from Harry Boone about @Liza joining a sync, and meeting notes from Lee Hao. A meeting notes widget is visible below the messages. The right sidebar shows channel details: 'Details #social-media', 'Add', 'Find', 'Call', 'More', 'About' (Topic: Track and coordinate social media, Description: Home of the social media team, Created on October 18th, 2019), 'Members' (21), and 'Organizations' (2).



---

2

# Methodology





## Virtual Machine Specs

- Three VMs
  - Ubuntu 20.04.3 LTS
    - Machine1, Machine2, Machine3 >> VMware Workstation
  - 4GB Ram
- File Setup
  - Direct Messaging
    - .jpg image
    - .txt document
  - Server Communications
    - .jpg image
    - .txt document





## Snapshots

- Volatile Memory
- 54 Total Snapshots
  - Base Snapshot
- Subset of snapshots where only one machine snapshotted, due to application restraints
  - Ex. Friend Requests





## Data Analysis

- Volatility 2.7
  - Process Memory
  - Linux\_pslist
    - Collected Discord / Slack PIDs
  - Linux\_dump\_map
    - zread()
      - Will write 0s for pages not present
    - read()
      - Skipped if the value was none





## Data Analysis

- Grepped files for subset of words:
  - Discord, discordapp, txt, username, password, slack, gmail, usernames
- Used the strings command to limit results to words with 4 or more characters
- Snapshots like : Quit Discord, used WxHexeditor





# Snapshots

Experiment	Snapshot	Account	Description
	Base Snapshot	All	A control snapshot that was made prior to the installation of Slack or Discord.
<b>Discord</b>	Install Snapshot	All	Snapshots were taken after Discord was installed using snap.
	Login Snapshot	All	Snapshots were taken after logging into Discord.
	Profile Image and Status Update Snapshot	All	Snapshots were taken after updating status message and user profile image.
	Friend Request Snapshot	Machine1	A snapshot was taken after the Friend Request Process was initiated. In this, Machine1 sent a friend request to Machine2 and Machine3.
	Friend Request Accepted Snapshot	Machine2/3	Snapshots were taken after accepting the Friend Request.
	Direct Messaging Snapshot	Machine1/2	Snapshots were taken after the direct message interaction between Machine1 and Machine2.
	Created Server Snapshot	Machine1	A snapshot was taken after the Machine1 account created a Discord Server.
	Joined Sever Server Snapshot	All	Snapshots were taken after Machine2 and Machine3 joined Machine1's Discord server and sent messages in general chat.
	Assigned Roles Snapshot	All	Snapshots were taken after Machine1 assigned roles to Machine2 and Machine 3.
	Added Role to Private Channel Snapshot	All	Snapshots were taken after Machine1 changed Machine's 3 role to see the hidden channel.
Voice Chat Snapshot	All	Snapshots were taken while Machine1 and Machine2 were in the General Voice chat channel.	
Quit Discord Snapshot	All	Snapshots were taken after each user quit Discord.	





## Snapshots

Slack	Install Snapshot	All	Snapshots were taken after Slack was installed using snap.
	Login / Create Workspace Snapshot	Machine1	A snapshot was taken after logging into Slack and creating a workspace.
	Login / Joined Slack Workspace Snapshot	Machine2/3	Snapshots were taken after Machine2 and Machine3 joined Machine1's workspace.
	Added Giphy Bot Snapshot	Machine1	A snapshot was created after Machine1 added the Giphy bot to the workspace.
	Updated Profile Snapshot	All	Snapshots were taken after updating status message and user profile image.
	Direct Chat Message Snapshot	All	Snapshots were taken after Machine1 sent direct messages to Machine2 and Machine3.
	Private Chat Snapshot	Machine1/2	Snapshots were taken after messages were sent in a private Chat.
	Private Chat Added Snapshot	All	Snapshots were taken after Machine3 was added to the private Chat.
	Quit Slack Snapshot	All	A snapshot was taken after each user quit Slack.





---

3

## Discord Results





## Discord - Install

Discord

Install Snapshot

All

Snapshots were taken after Discord was installed using snap.

- Reference to snap command



**VCU**



## Discord - Login

Login Snapshot

All

Snapshots were taken after logging into Discord.

- Username
- Email
- Password
- Discord ID
- Avatar ID
- Channel IDs
- Phone Numbers
- Last Timestamp
- Token
- Game Status
- Region
- Geolocation

```
"login": "jamesk654test@gmail.com",  
'password': REDACTED, "undelete":  
false, captcha_key": "P0_ey0UeXAt01J  
KV1QiLCJhbGciOiJIUzI1NiJ9.eyJwYXNza  
2V5IjoimUZqdEJlR2RQLlpmUWhIakdRemU3  
M1RFdXA3Ui9WZWtNL0RlM3JjZjZ2OW5jSDR
```

Figure 1: Machine1 Username Password, Password Redacted



**VCU**



## Discord - Profile Update

	Profile Image and Status Update Snapshot	All	Snapshots were taken after updating status message and user profile image.
--	--	-----	--

- URL created for the Avatar Image
  - Accessible, will discuss more later on
- Status message
  - Exact phrase, not within JSON



## Discord - Friend Request / Accepted

Friend Request Snapshot	Machine1	A snapshot was taken after the Friend Request Process was initiated. In this, Machine1 sent a friend request to Machine2 and Machine3.
Friend Request Accepted Snapshot	Machine2/3	Snapshots were taken after accepting the Friend Request.

- Data for each user
- Success messages for sending friend request



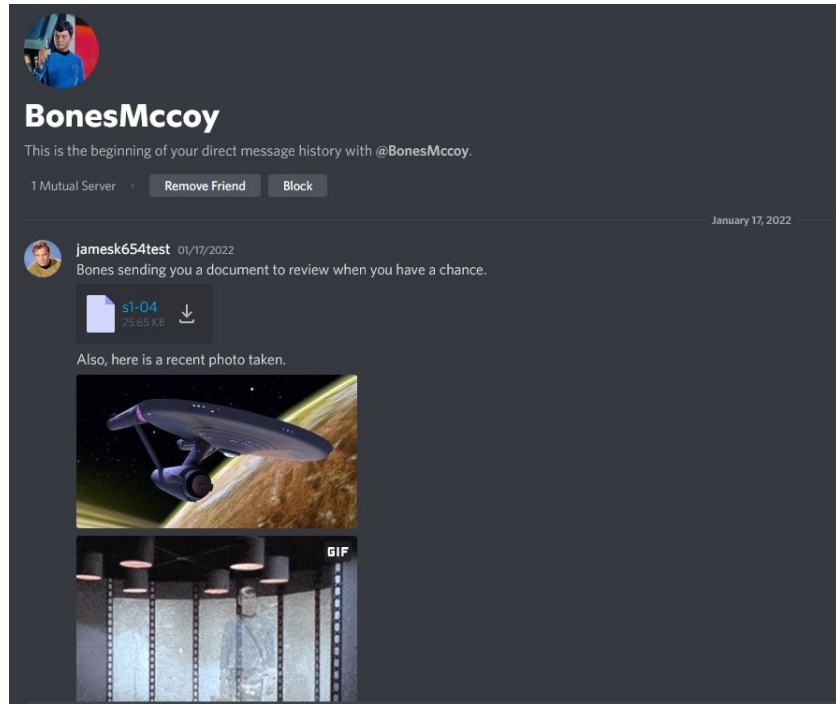


# Discord - Direct Messaging

Direct Messaging Snapshot

Machine1/2

Snapshots were taken after the direct message interaction between Machine1 and Machine2.



**VCU**

Computer Science  
College of Engineering



## Discord - Direct Messaging

Direct Messaging Snapshot

Machine1/2

Snapshots were taken after the direct message interaction between Machine1 and Machine2.

- Text URL
- Image URL

[https://\(cdn/media\).discordapp.com/\(avatars/attachments\)/id/file\\_id/file\\_name](https://(cdn/media).discordapp.com/(avatars/attachments)/id/file_id/file_name)

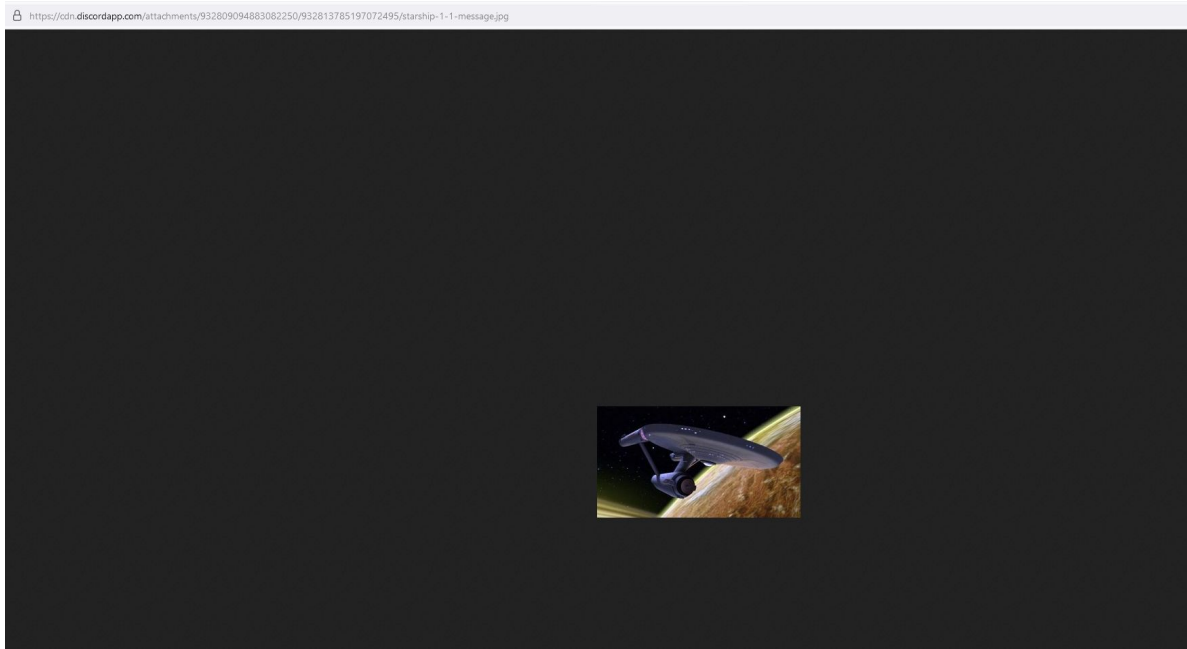
<https://cdn.discordapp.com/attachments/932809094883082250/932813785197072495/starship-1-1-message.jpg>



**VCU**



# Discord - Direct Messaging







## Discord - Created Server

Created Server Snapshot	Machine1	A snapshot was taken after the Machine1 account created a Discord Server.
-------------------------	----------	---

- Servername
- Guild ID
- Channels
- Icon





# Discord - Joined Server

The screenshot shows a Discord server interface for "The Enterprise Server" in the "# general" channel. The server has a dark theme. On the left sidebar, there are two text channels: "# general" and "# officers-only", and one voice channel: "General". The main chat area displays a welcome message: "Welcome to The Enterprise Server. This is the beginning of this server." dated January 17, 2022. Below this, there are two automated messages from "BonesMccoy" with a "Wave to say hi!" button. A user named "jamesk654test" has posted a message: "Thanks for joining everyone! Here is the final episode for review." followed by a file named "final\_episode\_discord\_server" (32/57 KB) and a video thumbnail of a man in a Star Trek uniform with his hands raised. The bottom of the screen shows the user "jamesk654test" with a message input field for "#general".





## Discord - Joined Server

Joined Sever Server All  
Snapshot

Snapshots were taken after Machine2 and Machine3 joined Machine1's Discord server and sent messages in general chat.

- Image URLs
- Uploaded File URLs
- Message Text
- Reactions
- GIFs
- Author Name
- Author ID

```
": "932837983483215872", "type": 0, "content":  
"https://tenor.com/view/agree-nod-yes-yes-yes-hmmm-star-trek-gif-  
11857294", "channel_id": "932820912808534030", "author": {"id":  
"932015586098163784", "username": "nyotauhura" "avatar":  
"58a742acf8200cead988c0bb009f9flf", "discriminator": "1273",  
"public_flags": 0}, "attachments": [], "embeds": [],  
"mentions": [], "mention_roles": [], "pinned": false,  
"mention_everyone": false, "tts": false, "timestamp":  
"2022-01-18T03:25:06.554000+00:00", "edited_timestamp": null,  
"flags": 0, "components": [], "nonce": "932837983059443712",  
"referenced_message": null}03:25:06 GMT
```





## Discord - Assigned Roles

Assigned Roles Snapshot	All
-------------------------	-----

Snapshots were taken after Machine1 assigned roles to Machine2 and Machine 3.

- Machine1/2
  - Message data
  - Roles
- Machine3
  - Reference to channel name
  - Roles





# Discord - Added Role to Private Channel

Added Role to Private Channel Snapshot

All

Snapshots were taken after Machine1 changed Machine's 3 role to see the hidden channel.

#officers-only

Welcome to #officers-only!  
This is the start of the #officers-only private channel.

[Add members or roles](#) [Edit Channel](#)

Captain Medical Communications

January 17, 2022

**jameak654test** 01/17/2022  
Went ahead and assigned roles to everyone. Let me know if I missed anyone

**BonesMccoy** 01/17/2022  
You missed adding the communications role to the officers only channel.

**jameak654test** 01/17/2022  
Thanks [@BonesMccoy](#) I've gone ahead and fixed the roles.

**nyotauhura** 01/17/2022  
Yep I can see now

+ Message #officers-only



## Discord - Added Role to Private Channel

Added Role to Private Channel Snapshot	All	Snapshots were taken after Machine1 changed Machine's 3 role to see the hidden channel.
--	-----	---

- Machine3 JSON data related to messages in the private channel





## Discord - Voice Chat

Voice Chat Snapshot

All

Snapshots were taken while Machine1 and Machine2 were in the General Voice chat channel.

- Single line “General (voice channel), 2 users
- No reference to users or duration



**VCU**



## Discord - Quit

Quit Discord Snapshot

All

Snapshots were taken after each user quit Discord.

- No new data, but previous information still remained



**VCU**



---

4

# Slack Results

---





## Slack - Install

Install Snapshot

All

Snapshots were taken after Slack was installed using snap.

- Reference to snap command



**VCU**

Computer Science  
College of Engineering



## Slack - Login / Create / Joined Workspace

Login / Create Workspace Snapshot	Machine1	A snapshot was taken after logging into Slack and creating a workspace.
Login / Joined Slack Workspace Snapshot	Machine2/3	Snapshots were taken after Machine2 and Machine3 joined Machine1's workspace.

- Slack routes through external login server
- Limits direct message to workspaces only
- Emails
- Timezone
- Display info
- Statuses
- Workspace Invite
- Workspace Names





## Slack - Added Giphy Bot

Added Giphy Bot Snapshot

Machine1

A snapshot was created after Machine1 added the Giphy bot to the workspace.

- Giphy is not default
- Bot ID
- Name
- Profile



**VCU**



## Slack - Updated Profile

Updated Profile Snapshot	All	Snapshots were taken after updating status message and user profile image.
--------------------------	-----	--

- Custom status
- Custom status duration
- Image URL






## Slack - Direct Chat Message

Direct Chat Message  
Snapshot

All

Snapshots were taken after Machine1 sent direct messages to Machine2 and Machine3.


 **Captain** 4:13 PM  
Hi Nyota, thanks for joining here is the document to review

4:13 s1-04 ▾

```
1 Title: Where No Man Has Gone Before
2 Stardate: 1312.4
3 Original Airdate: Sep 22, 1966
4
```

starship-1-1-message.jpg ▾



 **Nyota Uhura** 4:55 PM  
👉 Oh, hello!



**VCU**

Computer Science  
College of Engineering



## Slack - Direct Chat Message

Direct Chat Message  
Snapshot

All

Snapshots were taken after Machine1 sent direct messages to Machine2 and Machine3.

- File Uploads
- Message Data
- Channel Data
- File Links

[https://the-enterprise-corp.slack.com/?redir=%2Ffiles-tmb%2FT02UJ1FRX7U-F02UMAGGG4C-e09e01d758%2Fstarship-1-1-message\\_80.jpg](https://the-enterprise-corp.slack.com/?redir=%2Ffiles-tmb%2FT02UJ1FRX7U-F02UMAGGG4C-e09e01d758%2Fstarship-1-1-message_80.jpg)



**VCU**



# Slack - Direct Chat Message

https://the-enterprise-corp.slack.com/?redir=%2Ffiles-tmb%2FT02UJ1FRX7U-F02UMAGGG4C-e09e01d758%2Fstarship-1-1-1-message\_80.jpg

You need to sign in to see this page.



## Sign in to The Enterprise

the-enterprise-corp.slack.com

 Sign in with Google

 Sign in with Apple

OR

Email address

name@work-email.com

Password

Your password

Sign in

Forgot your password? [Get help signing in](#)

Looking for another workspace? [Find your workspaces](#)



**VCU**

Computer Science  
College of Engineering





## Slack - General Chat Messages

General Chat Message  
Snapshot

All

Snapshots were taken after messages were sent in the  
general chat.

- Timestamp
- Text
- Author
- Author Icon
- Author ID
- Author Link



**VCU**



## Slack - Private Chat

Private Chat Snapshot

All

Snapshots were taken after messages were sent in a private Chat.

- No roles
- JSON Message data on Machine 1 / Machine 2



**VCU**

Computer Science  
College of Engineering



## Slack - Private Chat Added

Private Chat Added Snapshot	All
--------------------------------	-----

Snapshots were taken after Machine3 was added to the private Chat.

- JSON message data was found after Machine 3 was added





## Slack - Quit Slack

Quit Slack Snapshot

All

A snapshot was taken after each user quit Slack.

- No new data, but previous information still remained



**VCU**

Computer Science  
College of Engineering

---

5

# Summary





## Summary

- JSON Data
- Discord upload links accessible
- Slack links restricted

Artifact	Discord	Slack
Avatar Image	x	x*
Discord Server	x	N/A
Email	x	x
Emojis	x	x
Friend Request	x	N/A
Gifs	x	x
Image	x	x*
Message	x	x
Password	x	-
Restricted Channels	-	-
Status	x	x
Slack Workspace	N/A	x
Text File	x	x*
User Roles	x	N/A
Username	x	x
Voice Chat	-	N/A



---

6

## Future Work





## Future Work

- Additional tests
  - Users Editing Messages
  - Users deleting messages, accounts
  - Users leaving discords
  - Administrators deleting messages
  - Pinned Messages
  - What data exists after prolonged usage
  - Screen sharing / Streaming
  - Discord Bots
  - Retrieving additional file types like videos
- Creating a framework to parse the json data and reconstruct messages







# Thanks!

*Any* **questions** ?

