Investigate Microsoft 365 Data

Task: *1 - Perform a content search for deleted emails/ Create an eDiscovery case*

In this exercise, you will use the content search to find emails with the keyword IP address.

1. Sign into Marguerite's account

2. Access Security and Compliance by selecting Show more, click on the scroll arrow twice to scroll down, select Security, select Office 365 Security and Compliance Center

3. Click **Permissions** from the left side menu.

4. Click the scroll arrow 3 time then Select the **eDiscovery Manager** role.

5. In the **eDiscovery Manager** section, click on **Edit role group**.

6. The Edit role group wizard opens. Click on **Choose eDiscovery Manager** tab. Click **Choose eDiscovery Manager**.

7. Click on **(+) Add**.

8. Select **Marguerite Ortiz** from the **Members** list and click **Add**.

9. Click **Done** and then **Save**. Click **close**.
10. Click on the scroll arrow until youfind Search
11. Click on Search
12. Click on Content Seach

13. Click **(+) Guided search** on the top menu.

14. Type **Content Search Test** into the **Name.**

15. Click **Next**

16. Select **All locations** and click **Next**.

17. Type **IP address** into the Keywords box and click **Finish**.

When the content search finishes, you will see all mailbox items that you may have created in this tenant. Since we issue blank tenants for the labs you may see nothing

18. Cancel Searches. Answer Yes to cancel the search.

Create an eDiscovery case

1. Click on the Permissions tab in your bowser address window at the top of the screen
2. Click on the scroll arrow twice
3. Click on eDiscovery

4. Click **(+) Create a case** on the top menu.

5. The New case wizard opens on the right side.

6. Click on the Next Navigation Tab to enter **IKP Address Violation(should be IP)** into the **Case name** field and click **Save**.

7. Back on the eDiscovery page, click **Open** on your case.

8. On the Core ED page, click on **Holds** from the top menu.

9. Click on **(+) Create** for a new Hold.

10. Click on the Next Navigation button to enter **IP Address Violation** into the **Name** field and click **Next**.

11. For the location **Exchange email**, click **Choose users, groups or teams**.

12. Click on **Choose users, groups or teams** again.

13. Enter **Ramiro** into the search field and click on the search icon. Scroll down to Select **Ramiro Armenta** from the search results.

14. Click **Choose** and **Done**.

15. Click **Next** in the wizard.

16. Enter **IP address** into the Keywords box press enter and click **Next**.

17. Click **Create this hold** on the Review your settings page.

18. On the Core ED page again, click on **Searches** from the top menu.

19. Click on **(+) New search.**

20. Enter **IP Address** into the **Keywords** field and select **Locations on hold** below **Locations**.

21. Click **Save the down arrow by Save and click Save**

22. Clcik on the Next navigation button to Enter **IP Address Violation** into the Name field and click **Save**.

You have now created an eDiscovery case with a configured hold and content search.