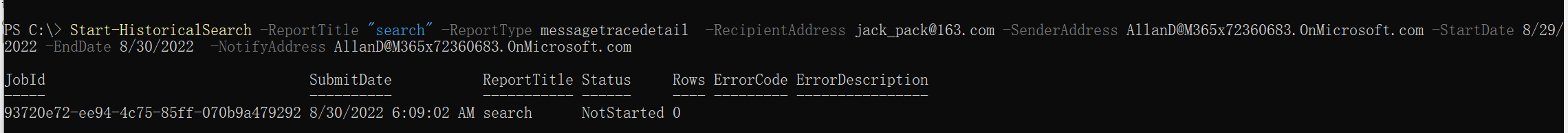
# Use history mail search (within 90days)

1. Use the following PowerShell command for filtering mail，after it is done , recipient email will be received a notification email with a report link,

Start-HistoricalSearch -ReportTitle "search" -ReportType messagetracedetail -RecipientAddress jack @163.com -SenderAddress AllanD@M365x72SS0683.OnMicrosoft.com -StartDate 8/29/2022 -EndDate 8/30/2022 -NotifyAddress [AllanD@M365x72SS0683.OnMicrosoft.com](mailto:AllanD@M365x72SS0683.OnMicrosoft.com)



Use the “Get-HistoricalSearch | fl “to view the file URL ，

Text

Description automatically generated

In the recipient mailbox will receive the relevant report information , please click the link for getting the report files.

Graphical user interface, application, Teams

Description automatically generated

1. Filtering the report files, filter by Event ID = Agent Info，

Graphical user interface, table

Description automatically generated

1. Date screening for Custom\_data,

Text

Description automatically generated

* DIR:OUT, spam confidence level(SCL) 5-9
* SFV = SPM, SCL >=1, DI=SO

If the above conditions are met , the message will be routed to HRDP（High Risk Delivery Pool），In this customer environment , we need to filter out spam > 5 mail message

# Use ATP Report for filtering（within 10 days，Spam informations）

Example : use the following command to filter out: the ATP Report information send by Alland, which can be adjusted according to the actual situation.

Get-MailDetailATPReport | Where-Object {$\_.direction -eq "Outbound" -and $\_.senderaddress -eq "Alland@M365x72000683.onmicrosoft.com"} |Export-Csv c:\20220831atp.csv -NoTypeInformation -Encoding utf8

Graphical user interface, application, table, Excel

Description automatically generated

The SPM Information will be filtered out through the ATP Report to submit to product group for analyzing.