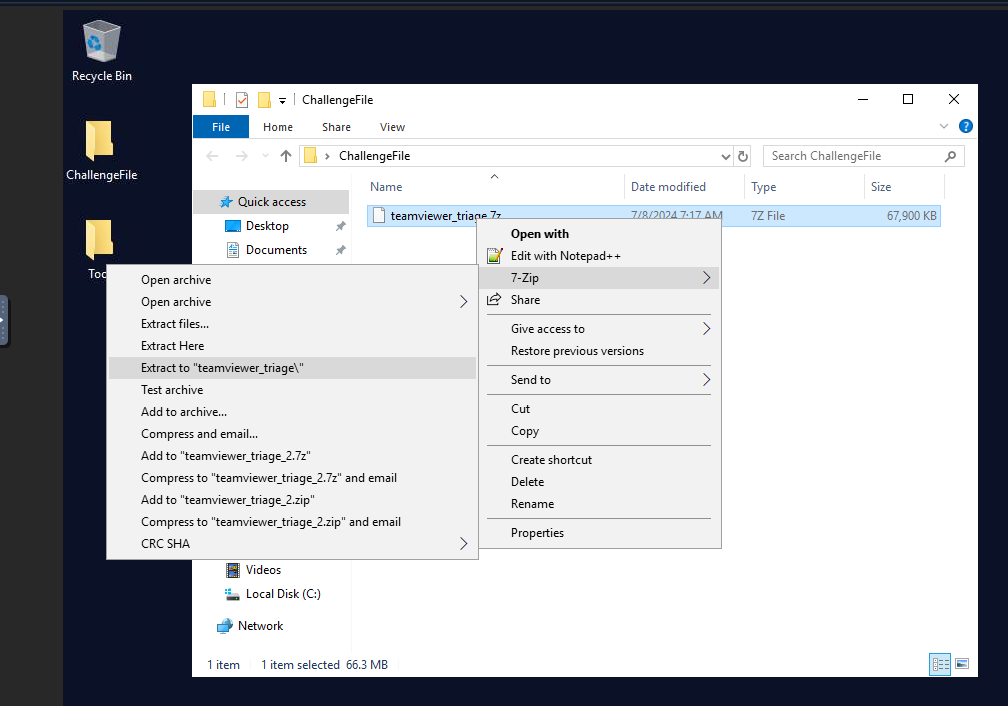
TeamViewer Forensics

During a workday, an employee noticed strange unauthorized activity on his computer, with applications opening and the mouse moving. Quickly realizing that someone was remotely accessing his machine via TeamViewer, the employee acted quickly, changing his TeamViewer password and alerting the security team. However, the employee must still clarify how the breach occurred and how far the threat actor has gone. Your challenge is to unravel this mystery and discover how the intruder gained access and what they did.

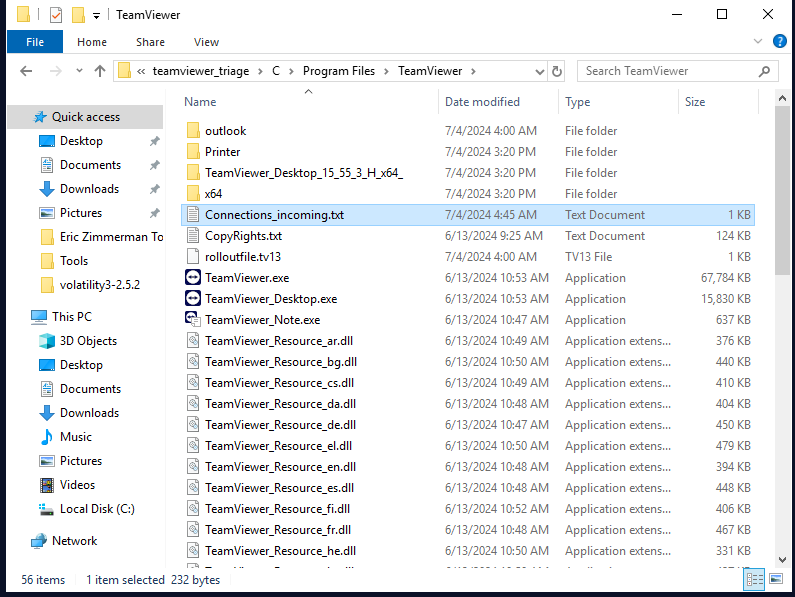
Step 1:

Extract the file.



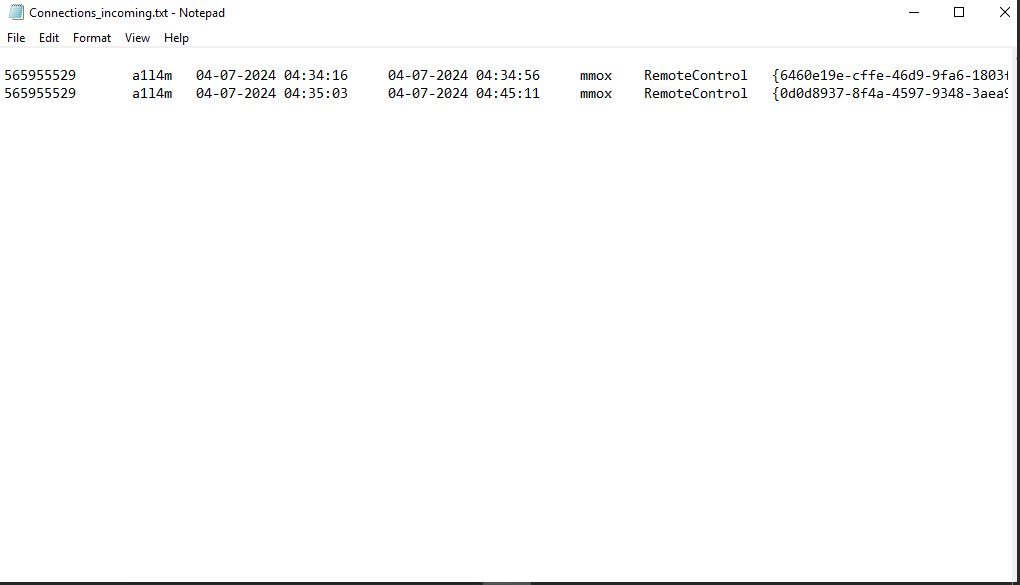
Step 2:

Open the file go to C/ProgramFiles/TeamViewer



Step 3:

Open the Connection\_incoming.txt then answer question number 1 and number 2.



Q1. What is the intruder’s username?

Top of Form

Ans: a1l4m

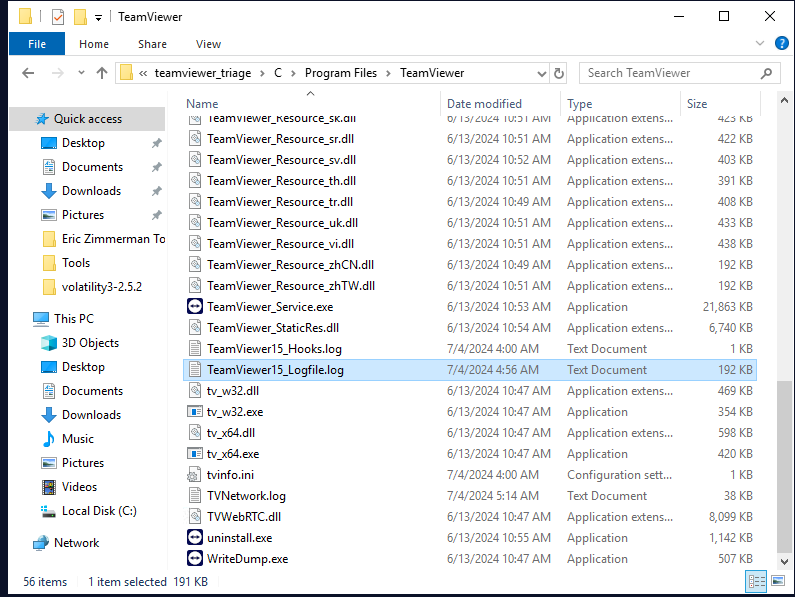
Q2. What is the “user ID” associated with the intruder's username?

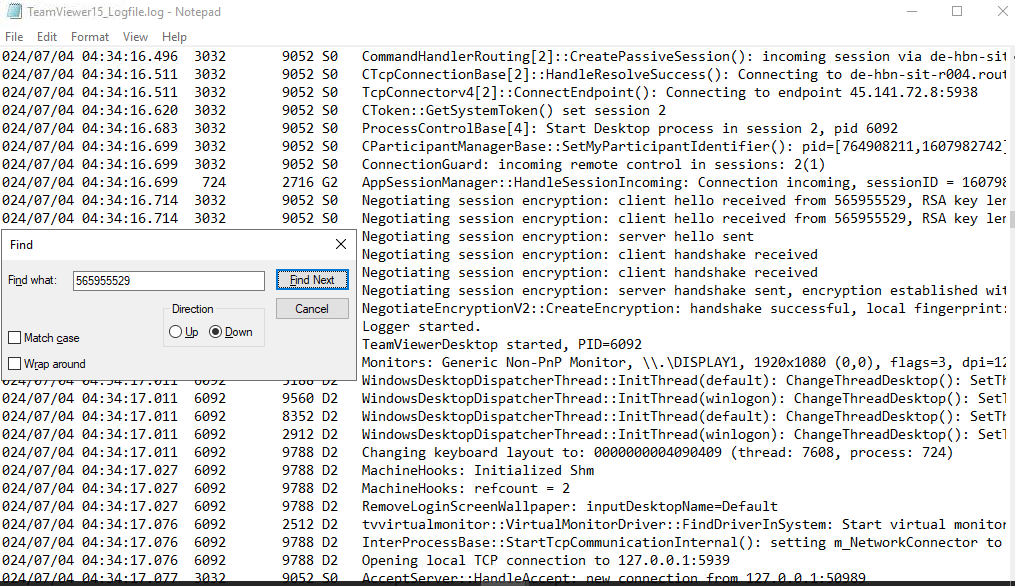
Top of Form

Ans: 565955529

Step 4:

In the same directory scroll down and look for “ TeamViewer\_Logfile ” open the file and use the user ID to answer question number 3.



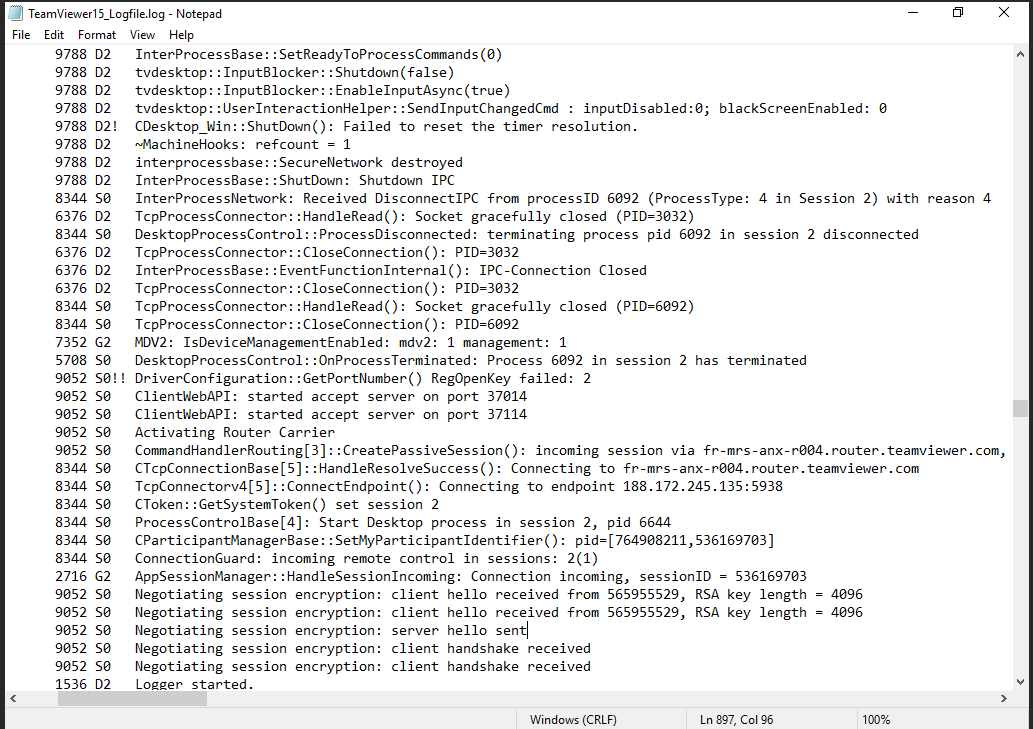


Q3. The attacker has joined more than one time. When did the intruder first access the victim's machine?

Ans: 2024-07-04 04:34:16.699

Step 5:

In the same file track the user activity and look for new session to answer the question number 4.

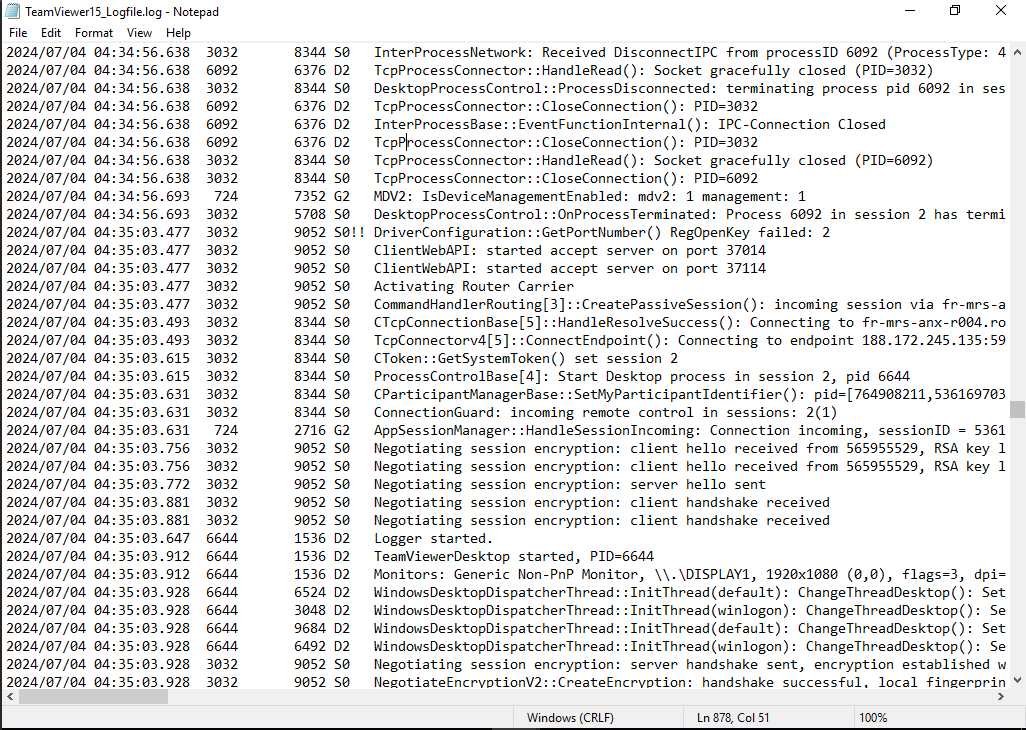


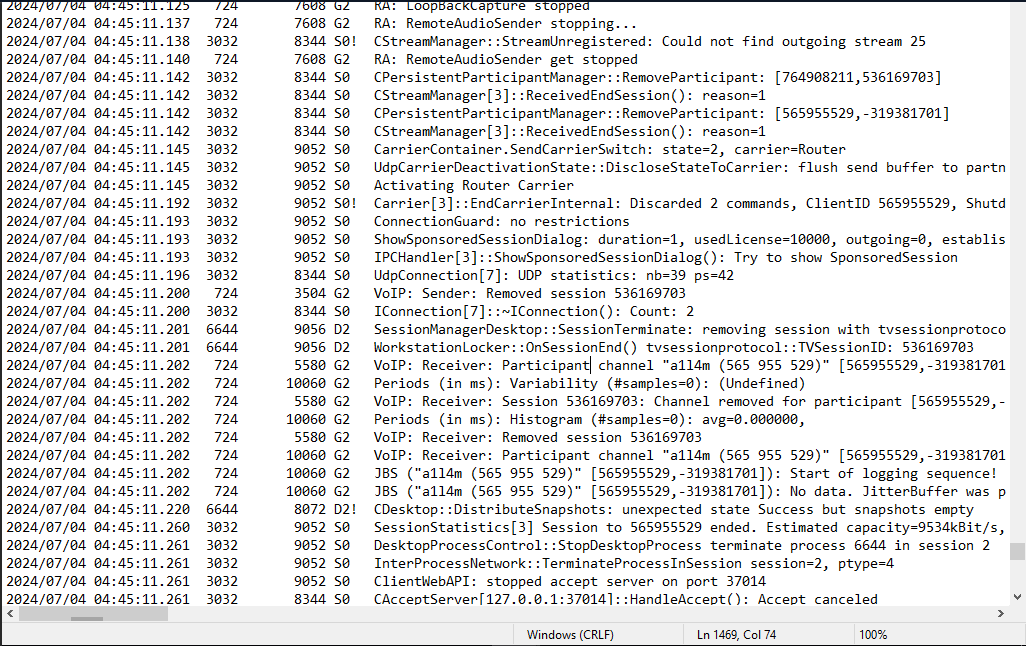
Q4. What is the “session ID” of the intruder's second access to the computer?

Ans: 536169703

Step 6:

In the same file look for 2ND session duration of intruder by using the session ID and subtract the timestamp of activities to answer question number 5.



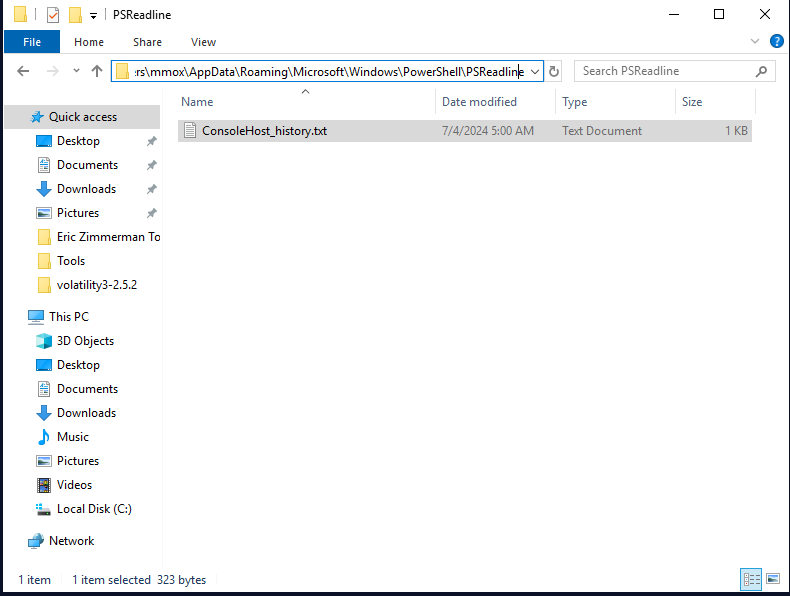


Q5. What was the duration of the second session in seconds.milliseconds?

Ans: 607.571

Step 7:

Change directory to C/user/mmox/AppData/Roaming/Microsoft/Windows/PowerShell/PSReadline then open the ConsoleHost\_history.txt to answer question number 6.





Top of Form

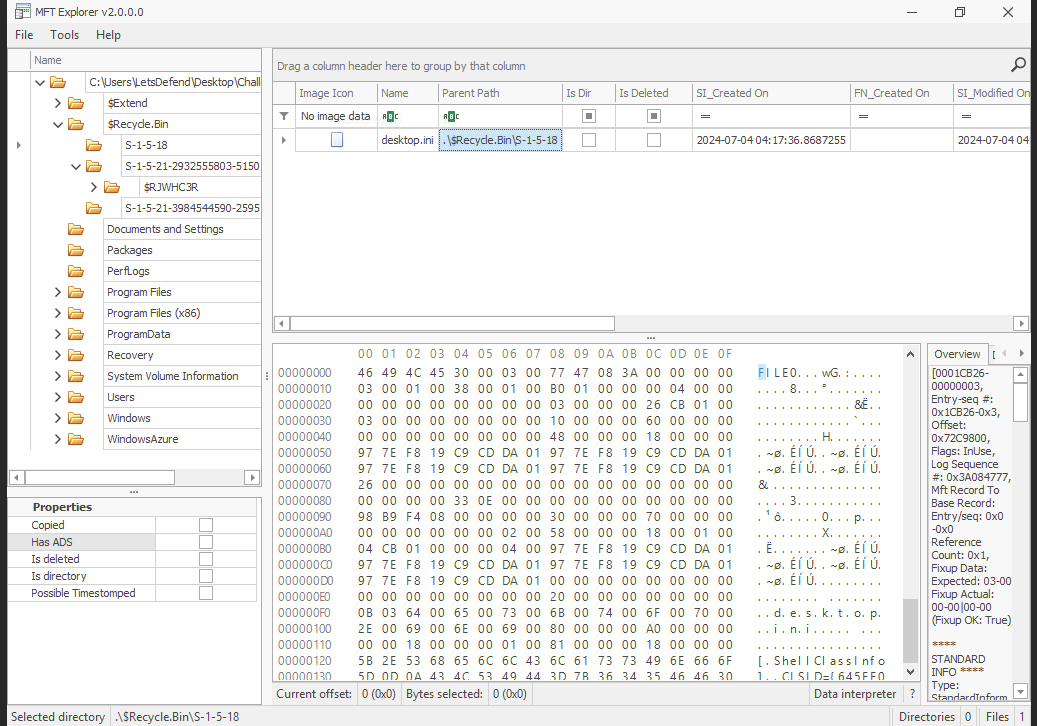
Q6. What is the IP address of the server to which the intruder exfiltrated data?

Top of Form

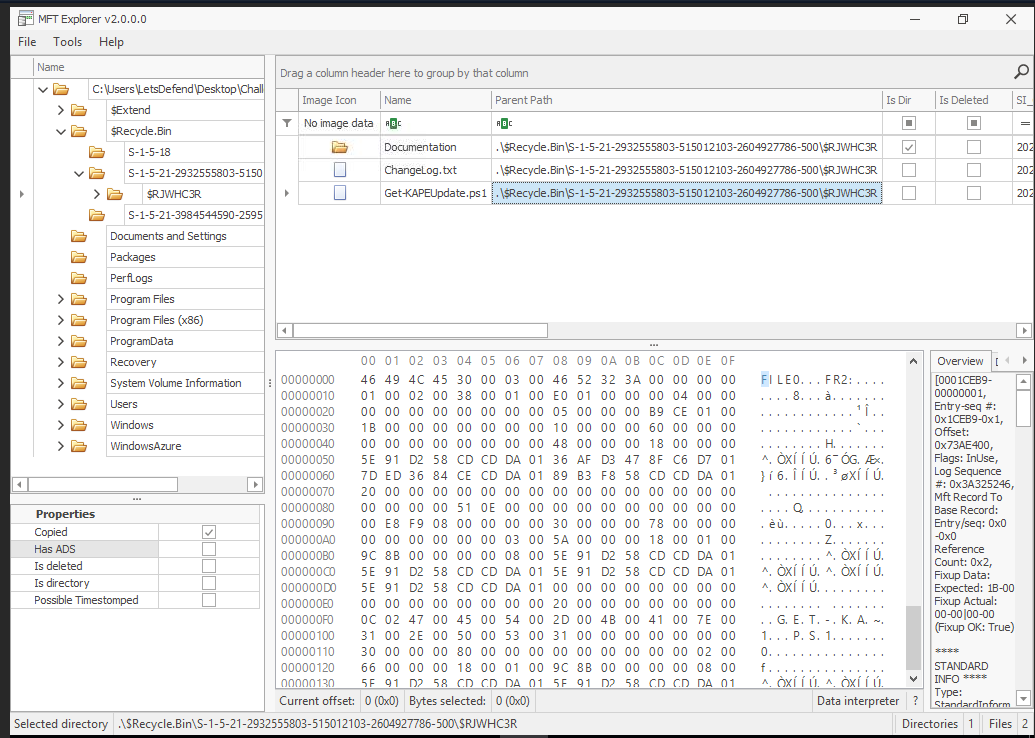
Ans: 116.203.186.178

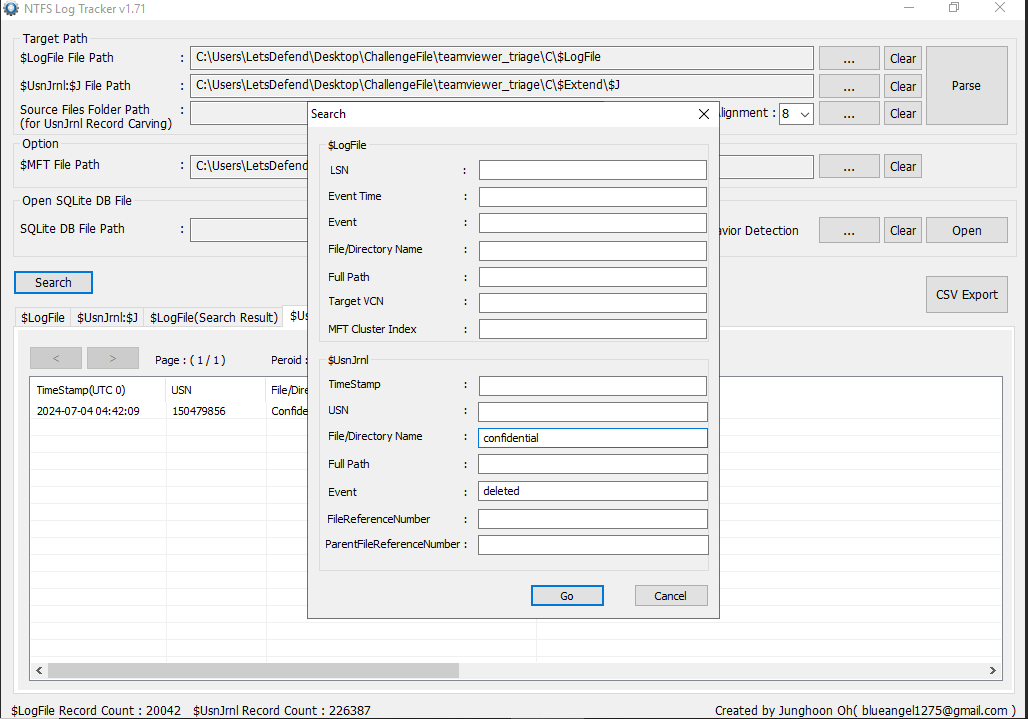
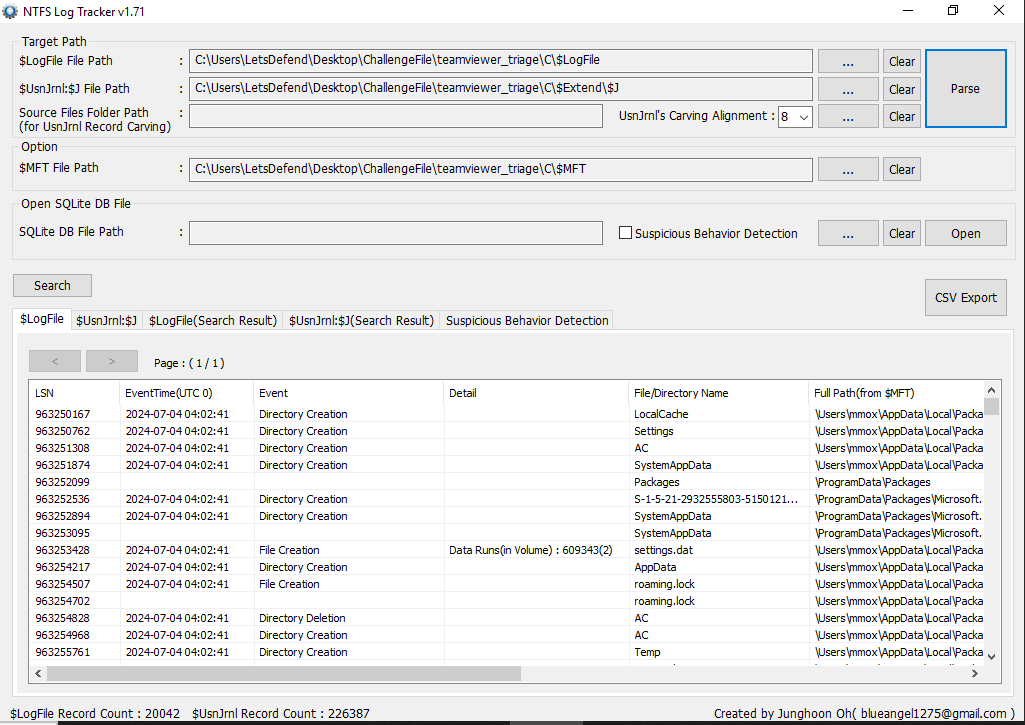
Step 8:

Use the Tools in the system like MFT explorer and Journal Tracker to answer question 7 and 8. Not sure in question 7 but here’s my findings using MFT explorer. (Reference in screenshot below)



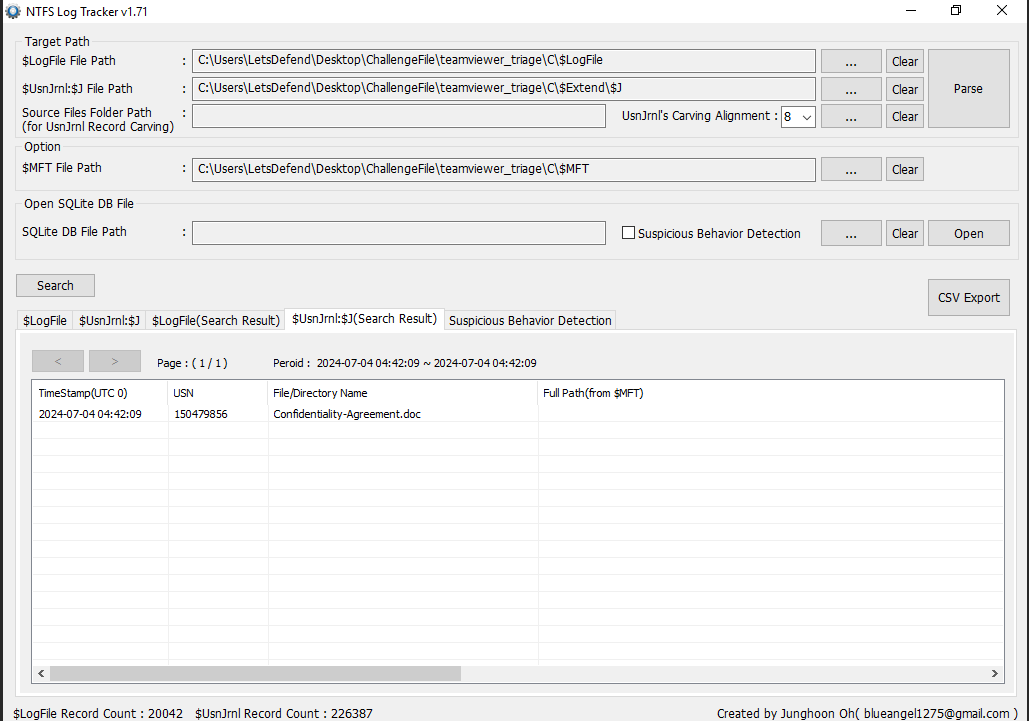
MFT – File exfiltrated count 3 based on findings





NFTS Log Tracker –

Use to look for confidential file timestamps deleted



Q7. How many files did the intruder exfiltrate?

Top of Form

Ans: 3

Q8. When did the intruder delete the confidential data from the system?

Ans: 2024-07-04 04:42:09

PS. Any corrections or suggestion will be much appreciated. Thank You