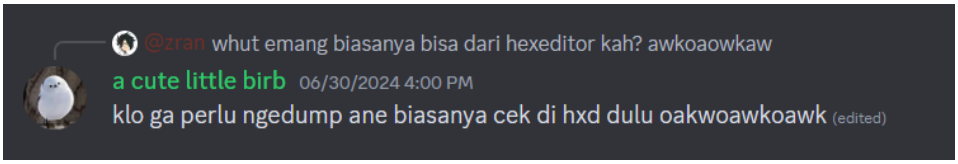
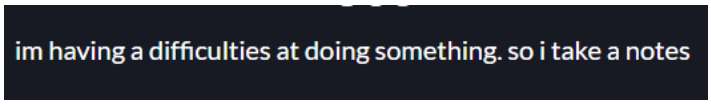
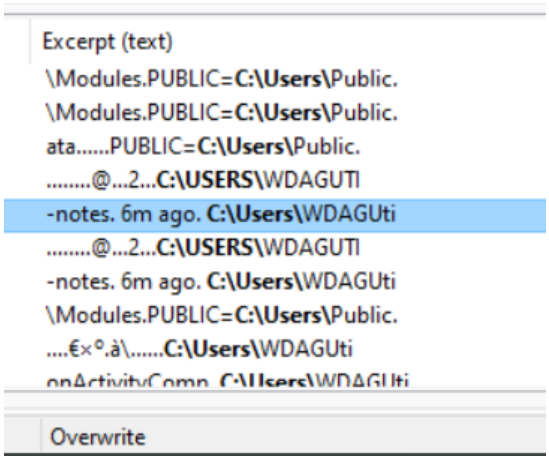


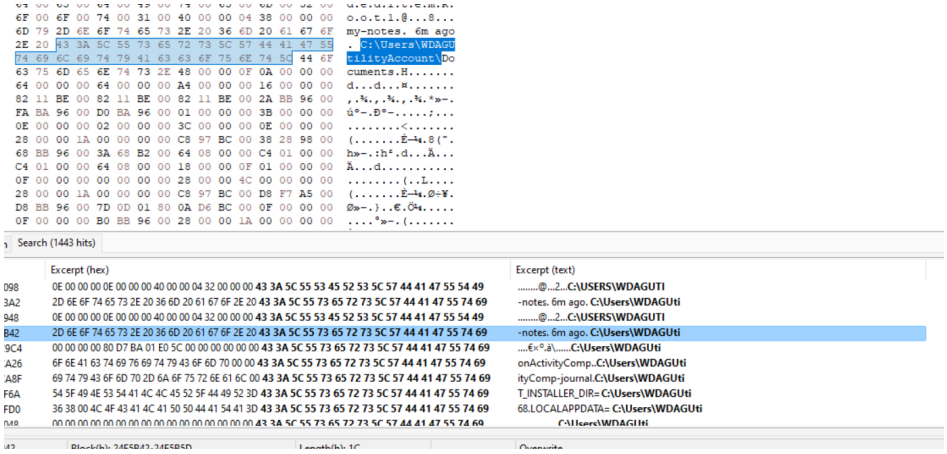
Gua pake HxD oakwoawkoakwoakw



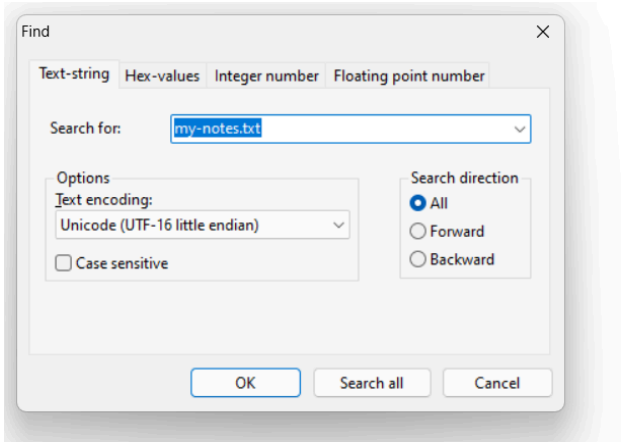
Dari chall dikasih tau kalau dia take a note (yes! What i mean is notepad!)
So the first step, is to look for the notepad activity. Cara pertama ane setiap ngerjain chall memdump yang berhubungan sama “file” adalah cari tau usernya dulu (biasanya pake plugin info, cuma karena di chall ini lu ga bisa pake vol, gua pake fitur search biasa)
Disini gua cek usernya pake cara search “C:\Users\”, dan ketika cari list user apa aja yg ada, bakal nemu user ‘WDAGUtilityAccount’ (yang mana merupakan user di Windows Sandbox)

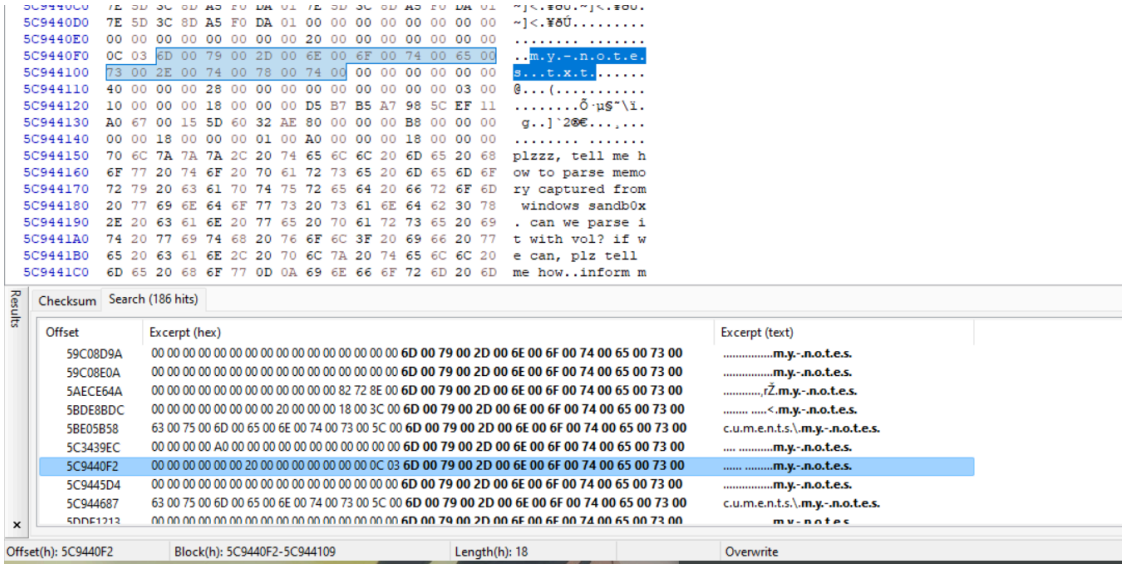


Dari pencarian user itu, lu bisa nemuin file yg dia punya apa aja, salah satunya my-notes (search dengan keyword “C:\Users\namauser\”)

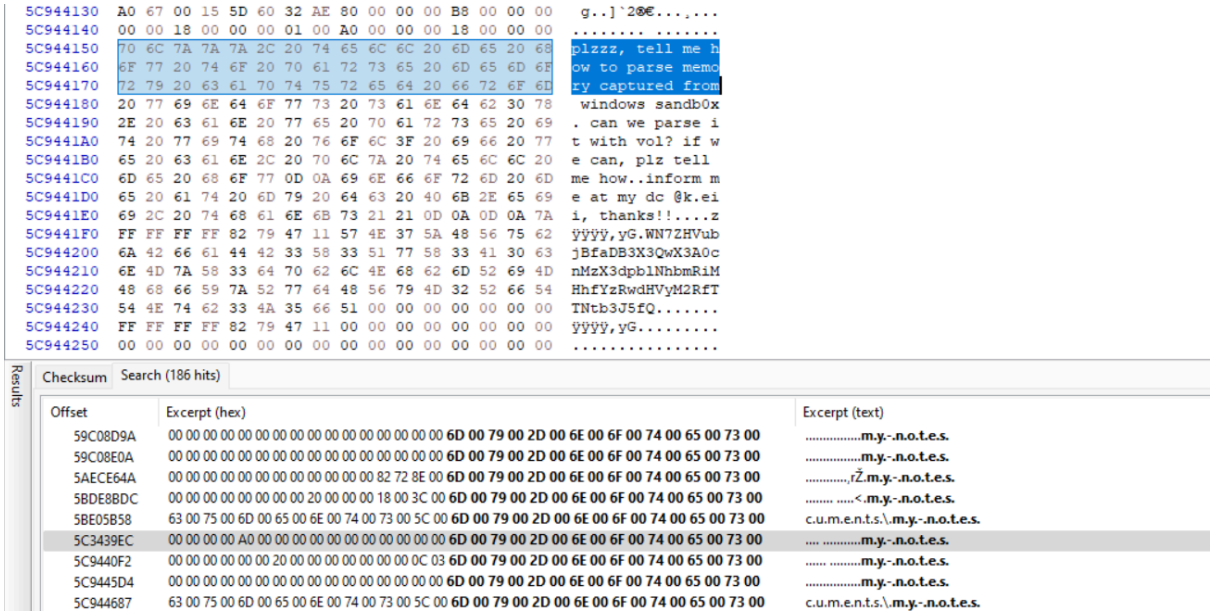


Simple sebenernya, lu tinggal cari file notenya, karena notepad itu pake UTF-16 little endian, setting searchnya gini (https://medium.com/@rifqiaramadhan/volatility-3-plugin-kusertime-notepad-sticky-evtxlog-f0e8739eee55)

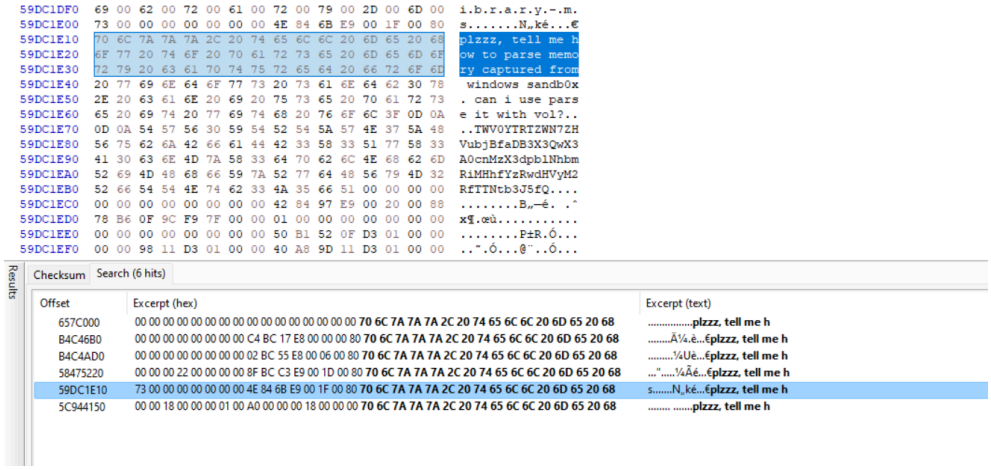




(tinggal nguli dikit lah 186 hit doang awikwok)



Coba search lagi disitu udah keliatan itu ada string base64 yg kayak kepadding? Corrupt?, dan di ss sebelumnya ada tulisan ‘6m ago’, filenya udah diedit ? mungkin gitu kali ya hehehe



Flag:
TWV0YTRTZWN7ZHVubjBfaDB3X3QwX3A0cnMzX3dpblNhbmRiMHhfYzRwdHVyM2RfTTNtb3J5fQ