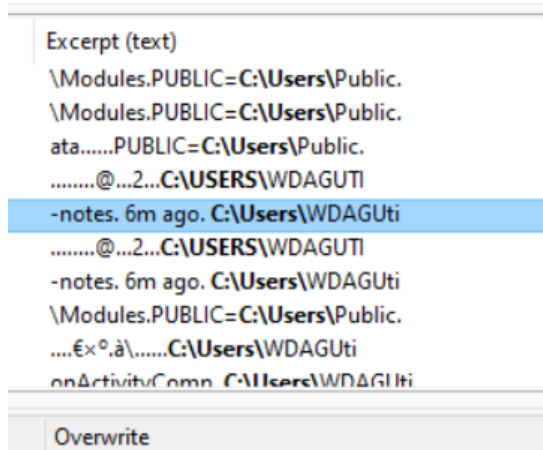


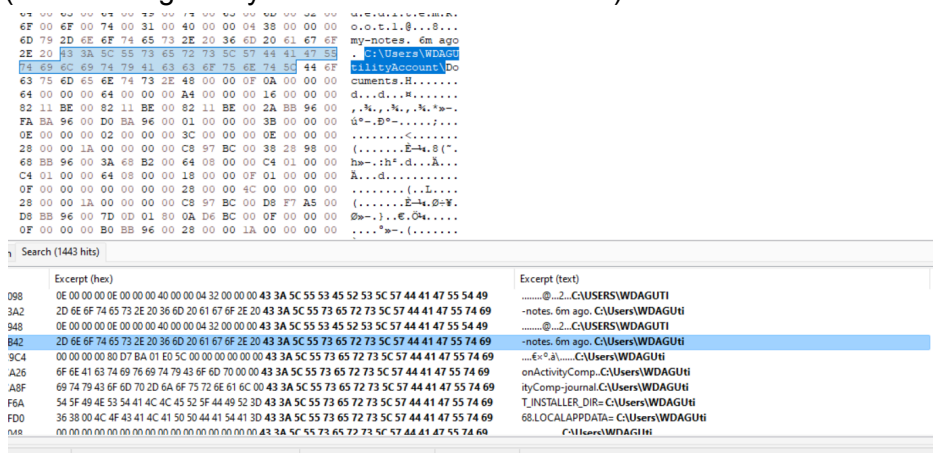
Gua pake HxD oakwoawkoakwoakw

im having a difficulties at doing something. so i take a notes

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)

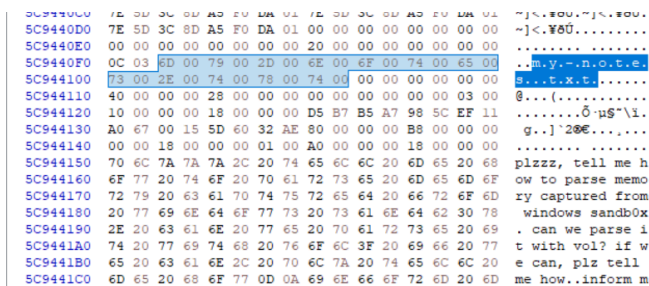


Dari pencarian user itu, lu bisa nemuin file yg dia punya apa aja, salah satunya my-notes (search dengan keyword "C:\Users\namuser")



Simple sebenarnya, 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>)



```

5C944130 A0 67 00 15 5D 60 32 AE 80 00 00 00 00 B8 00 00 00 g...j'20E.....
5C944140 00 00 18 00 00 00 01 00 00 00 00 00 18 00 00 00 .....
5C944150 70 6C 7A 7A 7A 2C 20 74 65 6C 6C 20 6D 65 20 68 plzzz, tell me h
5C944160 6F 77 20 74 6F 20 70 61 72 73 65 6D 6C 6D 65 6F ow to parse memo
5C944170 72 79 20 63 61 70 74 75 72 65 64 20 66 72 6F 6D ry captured from
5C944180 20 77 69 6E 64 6F 77 73 20 73 61 6E 64 62 30 78 windows sandbox
5C944190 2E 20 63 61 6E 20 77 65 20 70 61 6E 72 73 65 20 69 . can we parse i
5C9441A0 74 20 77 69 74 68 20 76 6F 6C 3F 20 69 66 20 77 t with vol? if w
5C9441B0 65 20 63 61 6E 2C 20 70 6C 7A 6E 74 65 6C 6C 20 e can, plz tell m
5C9441C0 6D 65 20 68 6F 77 0D 0A 69 6E 66 6F 72 6D 20 6D me how..inform m
5C9441D0 65 20 61 74 20 6D 79 20 64 63 20 40 6B 2E 65 69 e at my dc [k.e.i
5C9441E0 69 2C 20 74 68 61 6E 6B 73 21 21 0D 0A 0D 0A 7A i, thanks!!!!....
5C9441F0 FF FF FF FF 82 79 47 11 57 4E 37 5A 48 56 75 62 yyy,y.y.G.WX7ZWbu
5C944200 6A 42 66 61 44 42 33 58 33 71 57 58 33 41 30 63 jBTaB3xgWYK3A0oc
5C944210 6E 4D 7A 58 33 64 70 62 6C 4E 68 62 6D 52 69 4D nMzX3dpblNhbmmRIM
5C944220 48 68 66 59 7A 52 77 64 48 56 79 4D 32 52 66 54 HnFYeZWRHvHyM2RFT
5C944230 54 4E 74 62 33 4A 35 66 51 00 00 00 00 00 00 00 THt3rJs5fQ.....
5C944240 FF FF FF FF 82 79 47 11 00 00 00 00 00 00 00 00 yyy,y.yG.....
5C944250 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

Results

Checksum	Search (186 hits)	
Offset	Excerpt (hex)	Excerpt (text)
59C08D9A	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6D 00 79 00 2D 00 6E 00 6F 00 74 00 65 00 73 00my-.notes.
59C08BE0A	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6D 00 79 00 2D 00 6E 00 6F 00 74 00 65 00 73 00my-.notes.
5AECF64A	00 00 00 00 00 00 00 00 00 00 00 00 82 7E 8E 00 6D 00 79 00 2D 00 6E 00 6F 00 74 00 65 00 73 00iZ.my-.notes.
58DE8BDC	00 00 00 00 00 00 00 00 20 00 00 00 18 00 3C 00 6D 00 79 00 2D 00 6E 00 6F 00 74 00 65 00 73 00<.my-.notes.
5BE05B58	63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 5C 00 6D 00 79 00 2D 00 6E 00 6F 00 74 00 65 00 73 00	Comments.my-.notes.
5C439EC	00 00 00 00 A0 00 00 00 00 00 00 00 00 00 00 00 6D 00 79 00 2D 00 6E 00 6F 00 74 00 65 00 73 00my-.notes.
5C9440F2	00 00 00 00 00 00 20 00 00 00 00 00 00 00 0C 03 6D 00 79 00 2D 00 6E 00 6F 00 74 00 65 00 73 00my-.notes.
5C9445DA	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6D 00 79 00 2D 00 6E 00 6F 00 74 00 65 00 73 00my-.notes.
5C944687	63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 5C 00 6D 00 79 00 2D 00 6E 00 6F 00 74 00 65 00 73 00	Comments.my-.notes.

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

```

59DC1DF0 69 00 62 00 72 00 61 00 72 00 79 00 2D 00 6D 00 i.b.r.a.r.y.-m.
59DC1E00 73 00 00 00 00 00 00 00 4E 84 6B E9 00 1F 00 80 s.....N.ke...E
59DC1E10 70 6C 7A 7A 7A 2C 20 74 65 6C 6C 20 6D 65 20 68 plzzz, tell me h
59DC1E20 6F 77 20 74 6F 20 70 61 72 73 65 20 6D 65 6D 6F ow to parse memo
59DC1E30 72 75 20 63 61 70 74 75 72 65 64 20 66 72 6F 6B by captured from
59DC1E40 20 77 69 6E 64 6F 77 73 20 73 61 6E 64 62 30 78 windows sandb0x
59DC1E50 2E 20 63 61 6E 20 69 20 75 73 65 20 70 61 72 73 . can i use pars
59DC1E60 65 20 69 74 20 77 69 74 68 20 76 6F 6C 3F 0D 0A e it with vol?..
59DC1E70 0D 0A 54 57 56 30 59 54 52 54 5A 57 4E 37 5A 48 ..TWV0YTRTZWN7ZH
59DC1E80 56 75 62 6A 42 66 61 44 42 33 58 33 51 77 58 33 VubjBfaDB3X3QwX3
59DC1E90 41 30 63 6E 4D 7A 58 33 64 70 62 6C 4E 68 62 6D A0cnMzX3dpblNhbm
59DC1EA0 52 69 4D 48 68 66 59 7A 52 77 64 48 56 79 4D 32 RiMHhfYzRwdHVyM2
59DC1EB0 52 66 54 54 4E 74 62 33 4A 35 66 51 00 00 00 00 RfTTNtb3J5fQ....
59DC1EC0 00 00 00 00 00 00 00 00 42 84 97 E9 00 20 00 88 .....B...-é. ."
59DC1ED0 78 B6 0F 9C F9 7F 00 00 01 00 00 00 00 00 00 x%.æb.....
59DC1EE0 00 00 00 00 00 00 00 00 50 B1 52 0F D3 01 00 00 .....P±R.Ö...
59DC1EF0 00 00 98 11 D3 01 00 00 40 A8 9D 11 D3 01 00 00 ...".Ö...@".Ö...

```

Checksum	Search (6 hits)
Offset	Excerpt (hex)
657C000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 6C 7A 7A 7A 2C 20 74 65 6C 6C 20 6D 65 20 68
B4C46B0	00 00 00 00 00 00 00 00 C4 BC 17 E8 00 00 00 80 70 6C 7A 7A 7A 2C 20 74 65 6C 6C 20 6D 65 20 68
B4C4AD0	00 00 00 00 00 00 00 00 02 BC 55 E8 00 06 00 80 70 6C 7A 7A 7A 2C 20 74 65 6C 6C 20 6D 65 20 68
58475220	00 00 00 22 00 00 00 00 8F BC C3 E9 00 1D 00 80 70 6C 7A 7A 7A 2C 20 74 65 6C 6C 20 6D 65 20 68
59DC1E10	73 00 00 00 00 00 00 00 4E 84 6B E9 00 1F 00 80 70 6C 7A 7A 7A 2C 20 74 65 6C 6C 20 6D 65 20 68
5C944150	00 00 18 00 00 00 01 00 A0 00 00 00 18 00 00 00 70 6C 7A 7A 7A 2C 20 74 65 6C 6C 20 6D 65 20 68

Flag:
 TWV0YTRTZWN7ZHVubjBfaDB3X3QwX3A0cnMzX3dpblNhbmRiMHhfYzRwdHVyM2RfTTNtb3J5fQ