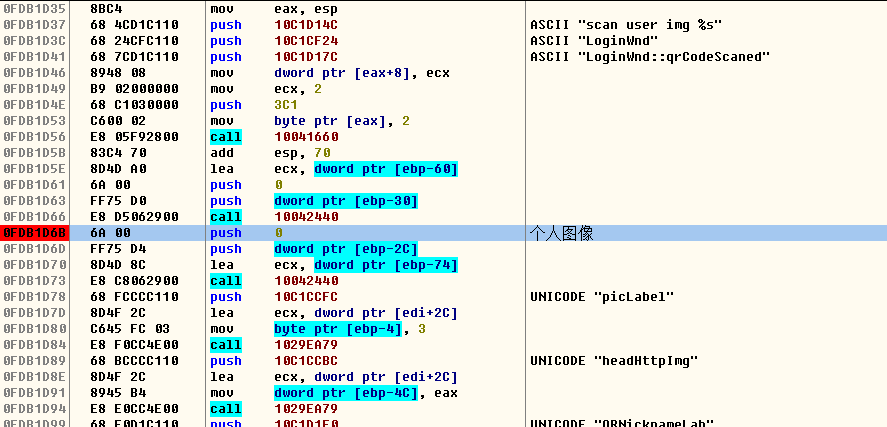
2.6.3.78版本分析：

登录前消息分析：

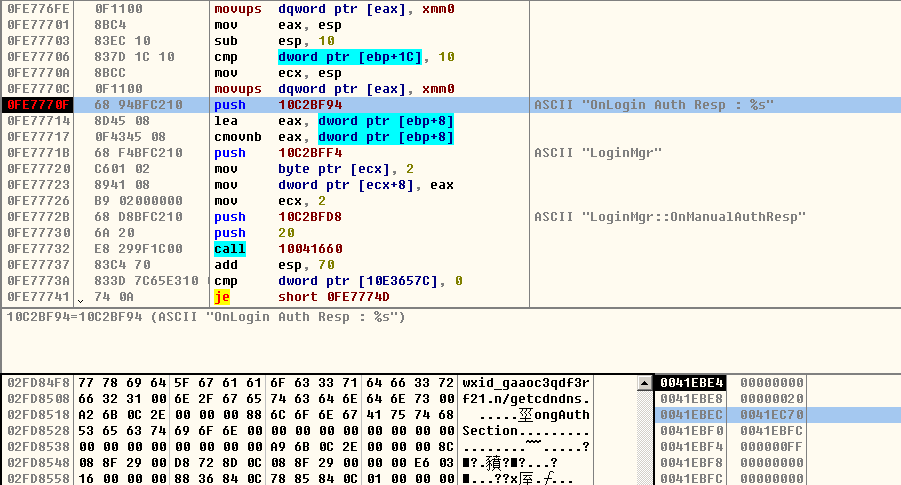
断点位置：WeChatWin.dll加载位置+0x1F1D6B



出现图像url

登录后：

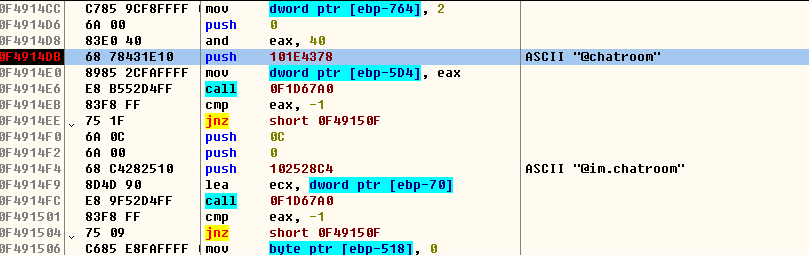
断点位置：WeChatWin.dll加载位置+0x2B770F



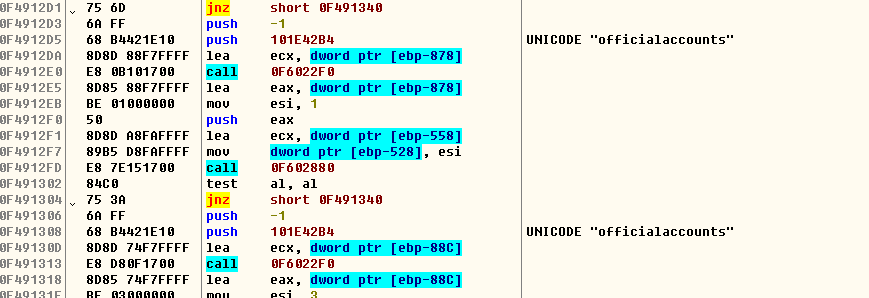
堆栈出现wxid，微信号

聊天-接收消息：

断点位置：WeChatWin.dll加载位置（0xf180000）+0x3114DB

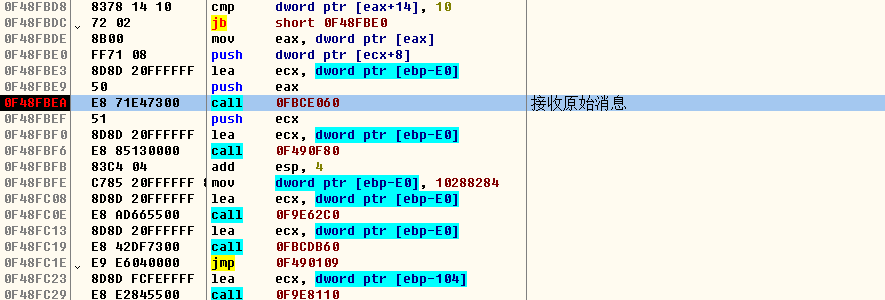


其上为



通过堆栈中数据，查找发送方，接收方信息。

接收原始消息位置：WeChatWin.dll加载位置(0xf180000)+0x30FBEA



此位置无太大特征，为聊天-接收消息位置栈回溯。