CAL POLY

California Cybersecurity
Institute

Computer Forensics CCIC Training

Chapter 11: Chat Logs

Lauren Pixley, Cassidy Elwell, and James Poirier

May 2019 (Version 2)

11

Chat Logs

Introduction

When you ran a keyword search earlier for Kenny McCormick, you found that a search result in the Skype main.db file. The Skype main.db file is used to store chat and contact information for the chat application Skype. It is always important to check chat artifacts because they show who the suspect was communicating with. Many chat programs also support file sharing, so you can see if the suspect shared or received any files through chat.

SkypeLogView

To view Craig's Skype chat logs, you are going to use a tool called SkypeLogView from Nirsoft. It can be downloaded from:

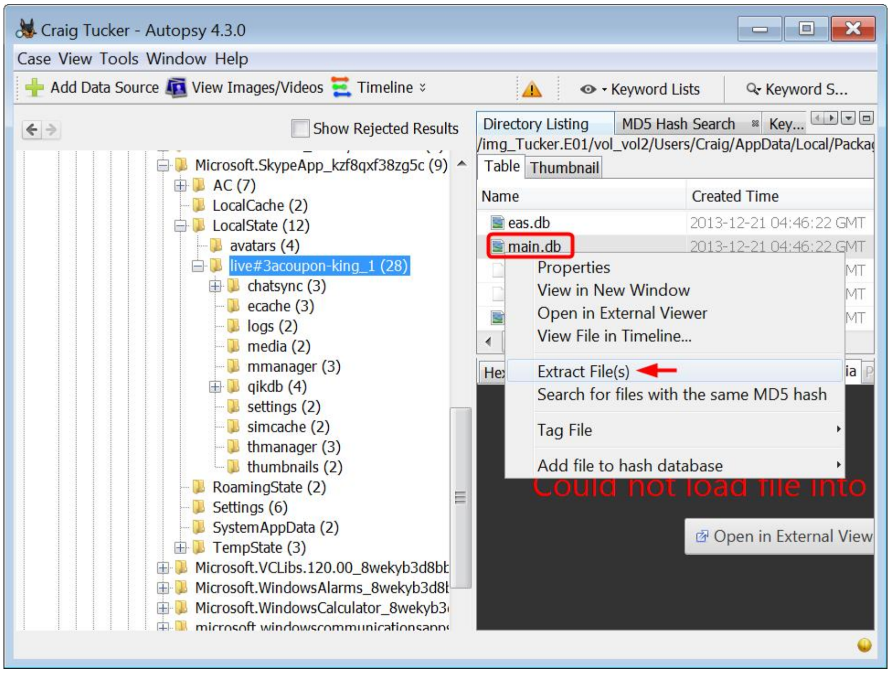
```
http://www.nirsoft.net/utils/skype_log_view.html
```

To use SkypeLogView, you need to export Craig's main.db file (see Figure 11-1). This is located in:

```
C:\Users\Craig\AppData\Local\Packages\Microsoft.SkypeApp_kzf8qxf38zg5c\
LocalState\live#3acoupon-king_1\main.db
```

Note: This location for the Skype database is specific to Windows 8. In Windows Vista and 7, it was located in:

```
C:\Users\[User Name]\AppData\Roaming\Skype\[Skype Name]
```

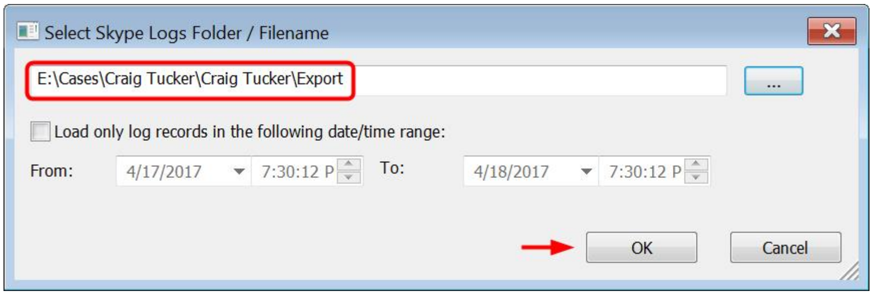


/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packag

Name	Created Time
eas.db	2013-12-21 04:46:22 GMT
main.db	2013-12-21 04:46:22 GMT

Figure 11-1 – Right-Click Craig's main.db File and Select Extract File(s)

Extract Craig's main.db file to your case Export folder. Open up the SkypeLogView tool. Either type in the location of your case Export folder or use the […] button to browse to your case Export folder. Click OK.



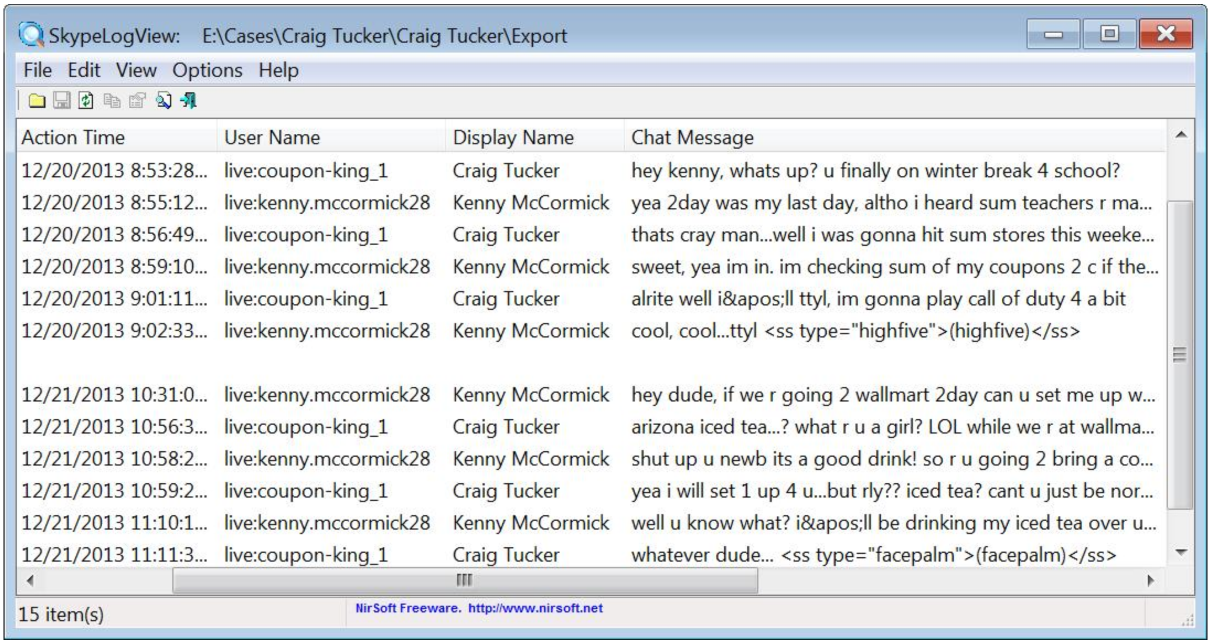
E:\Cases\Craig Tucker\Craig Tucker\Export

☐ Load only log records in the following date/time range:

From: 4/17/2017 7:30:12 P To: 4/18/2017 7:30:12 P

Figure 11-2 – Add Case Export Folder and Click OK

SkypeLogView will parse out all the Skype messages. It will also show who sent the chat message and when it was sent (see Figure 11-3).


SkypeLogView: E:\Cases\Craig Tucker\Craig Tucker\Export
File Edit View Options Help
15 item(s)
NirSoft Freeware. http://www.nirsoft.net

Action Time	User Name	Display Name	Chat Message
12/20/2013 8:53:28...	live:coupon-king_1	Craig Tucker	hey kenny, whats up? u finally on winter break 4 school?
12/20/2013 8:55:12...	live:kenny.mccormick28	Kenny McCormick	yea 2day was my last day, altho i heard sum teachers r ma...
12/20/2013 8:56:49...	live:coupon-king_1	Craig Tucker	thats cray man...well i was gonna hit sum stores this weeke...
12/20/2013 8:59:10...	live:kenny.mccormick28	Kenny McCormick	sweet, yea im in. im checking sum of my coupons 2 c if the...
12/20/2013 9:01:11...	live:coupon-king_1	Craig Tucker	alrite well i&apos;ll ttyl, im gonna play call of duty 4 a bit
12/20/2013 9:02:33...	live:kenny.mccormick28	Kenny McCormick	cool, cool...ttyl <ss type="highfive">(highfive)</ss>
12/21/2013 10:31:0...	live:kenny.mccormick28	Kenny McCormick	hey dude, if we r going 2 wallmart 2day can u set me up w...
12/21/2013 10:56:3...	live:coupon-king_1	Craig Tucker	arizona iced tea...? what r u a girl? LOL while we r at wallma...
12/21/2013 10:58:2...	live:kenny.mccormick28	Kenny McCormick	shut up u newb its a good drink! so r u going 2 bring a co...
12/21/2013 10:59:2...	live:coupon-king_1	Craig Tucker	yea i will set 1 up 4 u...but rly?? iced tea? cant u just be nor...
12/21/2013 11:10:1...	live:kenny.mccormick28	Kenny McCormick	well u know what? i&apos;ll be drinking my iced tea over u...
12/21/2013 11:11:3...	live:coupon-king_1	Craig Tucker	whatever dude... <ss type="facepalm">(facepalm)</ss>

Figure 11-3 - Parsed Skype Messages in SkypeLogView

If you click Edit►Select All and then File►Save Selected Items, you can save these messages to an html, csv, or txt report. As you can see through these logs, Kenny had asked Craig to get him the Arizona Iced Tea coupon.