



**ICAC TASK FORCE**

## Yahoo Messenger

### As An Investigative Tool

---

---

---


---

---

---

---

---



**ICAC TASK FORCE**

## Webinar Information

- All attendees will be muted.
- If you desire to ask a question you should use the questions section of the goto webinar dialogue box typically in the upper right corner of the screen.
- The questions will either be answered directly by a panelist or asked to the presenter who will answer.

---

---

---


---

---

---

---

---



**ICAC TASK FORCE**

- Questions will be answered at the end of each section and at the end of the webinar.
- Poll questions may be asked during the webinar. They will be left open only a short period of time, so please respond ASAP.
- At the conclusion of the webinar, a short survey will appear. Please complete it before signing off.
- Powerpoint will be made available to you.
- Within a few hours after the webinar an email with the link to the Powerpoint and access to the recorded session will be sent to you.

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

## Agenda

- Review of basic functions
- Aliases, video conferencing, web client
- Archiving vs Conversation History
- How do these changes impact our UC investigations?

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

## Basic IM

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

## Photo Sharing

- During photo sharing, more than one image can be sent at the same time
- Click **SAVE** to download the file and save it to your computer
- Remember to select the full size image

This window shows what the suspect is viewing  
 If the suspect is saying something sexual in the chat and looking at an image that is CP you will want to document the correlation

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

## Receiving a file

- Receiving a file via direct send method
- Run NETSTAT or GRABSTAT to identify the suspect's IP address

---

---

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

## File Transfer

- Direct file transfer
- This transfer is not archived
- Use screen capture software to document the transfer

---

---

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

## Webcam

---

---

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

### Best Bets to Capture IP

- Webcam/P2P
- File Transfer
- Photo Sharing (saving full file only)

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

### Webcam vs. Video Call

- YM 10 and above replaced webcam with video call
- This is a video conference which includes voice chat
- Initiating a video call activates your cam and microphone
- Accepting a video call does the same thing!

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

### Webcam vs. Video Call

- Webcams can be broadcast to multiple viewers –video call is one-on-one
- Webcam alone is still available
- Actions → More Actions
- Disable mic and webcam prior to UC chat sessions!

---

---

---

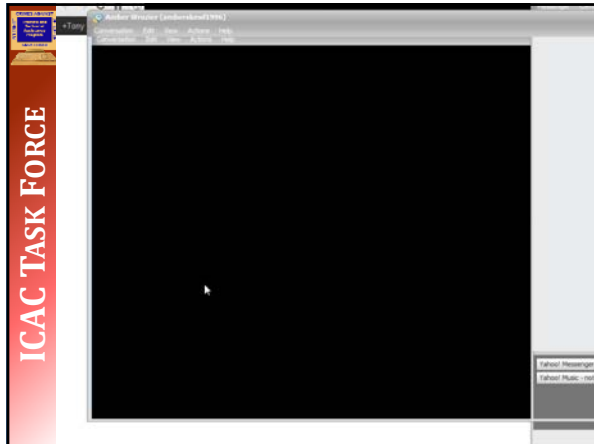
---

---

---

---

---



---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

### Aliases

- An alias allows you to send and receive messages under another name
- The alias is linked to your main screen name
- Other users will see you only as the alias name
- Alias name must be unique
- Requires logout/login to activate

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

### Aliases

- You can use aliases to pretend to be two people, e.g., parent and child, two friends, etc
- You can also enter a chat room using your alias
- Alias name is closely linked, showing the same icon pic, availability, etc.
- You can link multiple aliases to your screen name

---

---

---

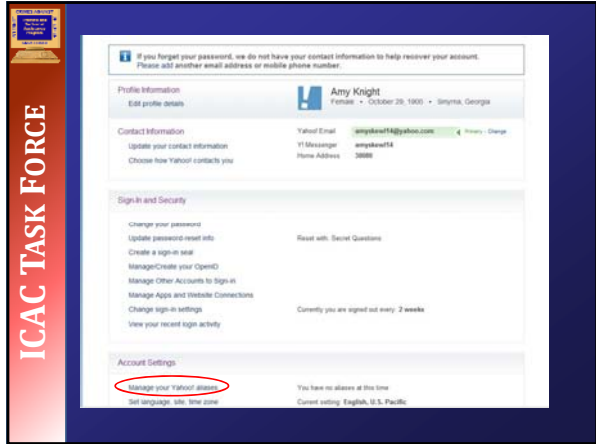
---

---

---

---

---



---

---

---

---

---

---

---

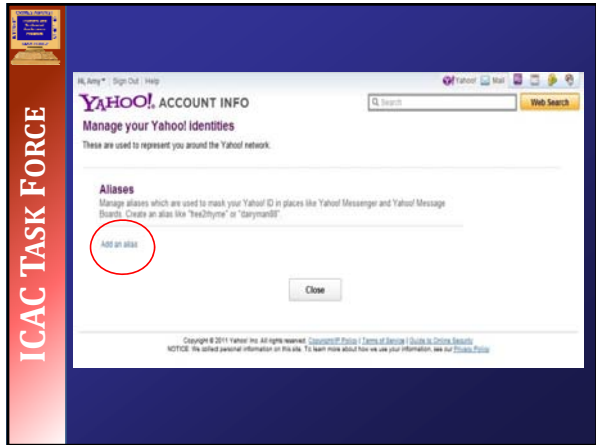
---

---

---

---

---



---

---

---

---

---

---

---

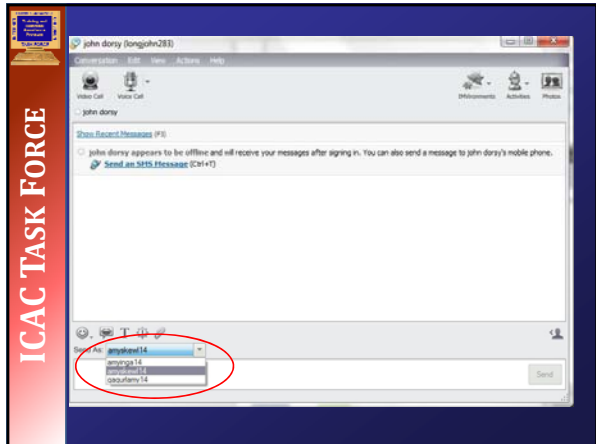
---

---

---

---

---



---

---

---

---

---

---

---

---

---

---

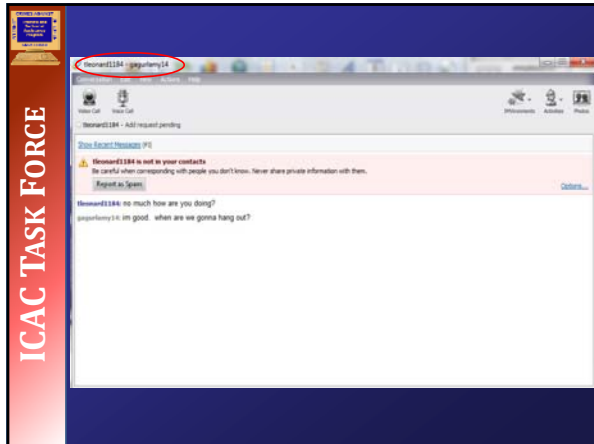
---

---

ICAC TASK FORCE

ICAC TASK FORCE

ICAC TASK FORCE



## Aliases

- An alias is a great tool, but can lead to problems if you aren't careful!
- Your alias doesn't have a separate email, icon pic or availability status
- If you display or change your icon, it changes for the alias as well = busted!
- It may show your "real" name if you add to Contacts
- Email address can give you away!

---

---

---

---

---

---

---

---

---

---

---

---



---

---

---

---

---

---

---

---

---

---

---

---



---

---

---

---

---

---

---

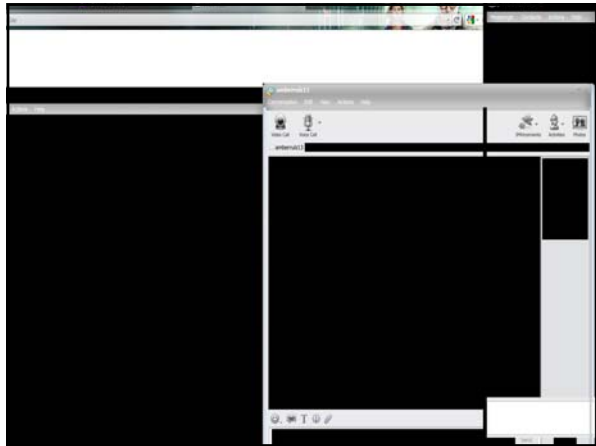
---

---

---

---

---



---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

### Web-Based YM

- In addition to the installed YM client, Yahoo also has a web-based version
- This allows users to chat directly from their mailbox
- No software has to be downloaded or installed
- These chats will not be archived if you have that function enabled in YM 10 or below
- You can log into YM and the web client at the same time

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

---

---

---

---

---

---

---

---



**ICAC TASK FORCE**

### Archiving Basics

- Archiving is a function available in YM 10 and below
- It can save all your chats on your local computer
- Must be enabled on each screen name and each computer
- Saves entire chat with date/time stamps
- Default setting is to purge files at logout

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

### Archiving Basics

- Chats are saved in a .DAT file format
- DAT files require special tools to alter or edit
- YM archive files also require a decoder to view/read outside of YM
- This makes the DAT file our "best evidence" for court purposes-system generated, complete, and secure

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

### File Structure Yahoo Chat Archive

<p>Vista Windows 7 (U.A.C. on)</p> <p>C:\</p> <ul style="list-style-type: none"> <li>\Users</li> <li>\User Name</li> <li>\AppData</li> <li>\Local</li> <li>\VirtualStore</li> <li>\Program files</li> <li>\Yahoo</li> <li>\Messenger</li> <li>\Profiles</li> <li>\UC Screen Name</li> <li>\Archive</li> <li>\Conferences or Messages</li> <li>\Screen Name of Offender</li> </ul>	<p>Windows XP and Earlier Versions Vista/7 (U.A.C. off)</p> <p>C:\</p> <ul style="list-style-type: none"> <li>\Program files</li> <li>\Yahoo</li> <li>\Messenger</li> <li>\Profiles</li> <li>\UC Screen Name</li> <li>\Archive</li> <li>\Conferences or Messages</li> <li>\Screen Name of Offender</li> </ul>
---	---

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

## Conversation History

- Yahoo 11 automatically saves copies of all your chats
- This used to be called "archiving" but is now called "conversation history"
- These chat logs are stored on Yahoo's servers and used for data mining
- Conversation history is on by default, and available from all computers and via email

---

---

---

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

## Conversation History

- Includes all date/time stamps and emoticons
- Allows chats to be saved locally in a text (.txt.) format only (no emoticons)
- Includes a record of voice calls, video calls, SMS, and conference messages
- Local configuration not is required for this feature
- Creates periodic updates, so chats are broken up, and may not be immediately available

---

---

---

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

The screenshot shows the Yahoo Conversation History interface. At the top, there's a search bar and a 'Set Up Voicemail' button. Below that is a table of conversations with columns for PARTICIPANT, SUBJECT, and DATE. The selected conversation shows a chat log with messages from 'stingnet4' and 'stingnet7'. A red circle highlights the email address 'stingnet7@yahoo.com' in the chat log.

---

---

---

---

---

---

---

---

---

---

---



---

---

---

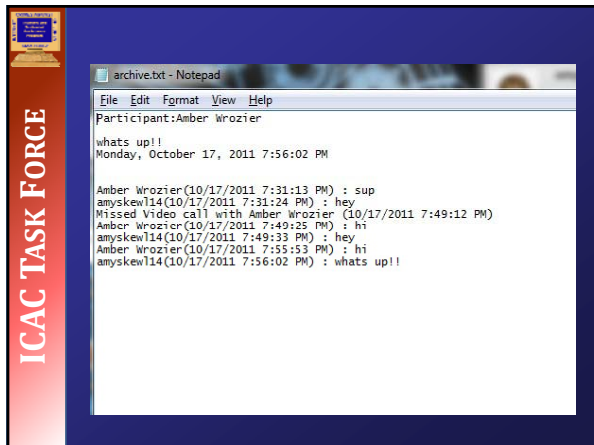
---

---

---

---

---



---

---

---

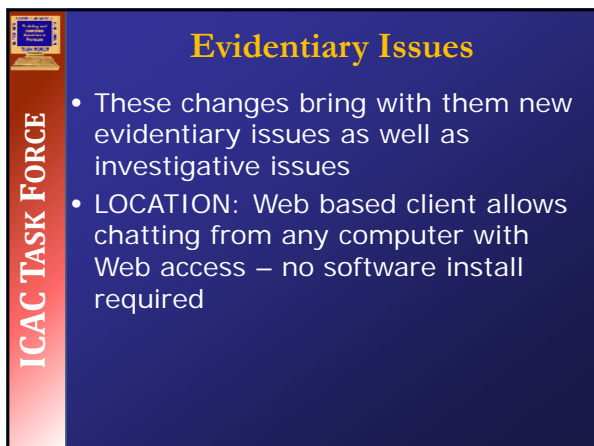
---

---

---

---

---



---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

### Evidentiary Issues

- FORMAT: No more DAT files to keep as evidence.
- Text files are not secure, and may not be complete (time stamps, etc.)
- Some courts won't accept copy-and-paste
- How do you save your chats now?
- How will you save them with YM 11?
- Camtasia, SnagIt, Yahoo records

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

### Investigative Issues

- Conversation History = more evidence than before
- No more concern about archiving on suspect's computer – his chats are saved!
- His entire YM chat history will be available with a search warrant, including connection records of video and voice chats

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

### Investigative Issues

- Good news: tons of pattern evidence, and more victims identified
- Bad news: tons of pattern evidence, and more victims identified
- What will this do to your workload per case?
- Multiple subpoenas/search warrants, multiple interviews, multiple referrals
- No more "It was just this once" defense

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

### Investigative Issues

- Next Issue –Privacy
- Can we obtain all chat logs or only certain ones?
- Can we review all chat logs for evidence?
- Will additional SW be required?
- Consult your prosecutor!

---

---

---

---

---

---

---

---

**ICAC TASK FORCE**

Capt. Tony Leonard  
Smyrna, GA Police Dept.  
678-631-5106  
tleonard@ci.smyrna.ga.us

---

---

---

---

---

---

---

---