

Authenticate

User Guide

Version 1.0.7

Disclaimer

Care has been taken in assuring the information contained in this manual is correct but the author, developer and any individual, associated company, distributor or reseller do not accept responsibility for errors or omissions.

In no event shall the aforementioned parties be liable for any loss of profit or any other commercial damage including, but not limited to, special, incidental, consequential or other damages arising from the provision of this document.

Independent legal advise should be sort regarding the evidentiary value of this document and or recordings stored in the *.IMG and *.IM2 formats.

Table of Content

1	<i>Authenticate Software</i>	3
1.1	<i>Computer Hardware Requirements</i>	3
1.2	<i>Installing Authenticate</i>	3
2	<i>Running Authenticate</i>	4
2.1	<i>Authenticate Main Window</i>	4
2.2	<i>Authenticate Version</i>	4
2.3	<i>Loading Audio Files</i>	5
2.3.1	<i>Audio File Details</i>	6
2.4	<i>Main Window Descriptions</i>	7
2.4.1	<i>Current Packet Information</i>	7
2.4.2	<i>Summary of Authentication Results</i>	7
2.4.3	<i>Summary of the Most Common Irregularities</i>	7
2.4.4	<i>Waveform and Authentication Processing Information</i>	8
2.4.5	<i>Replay Controls</i>	8
2.5	<i>Authenticating Audio Files</i>	9
3	<i>File Integrity</i>	10
3.1	<i>Integrity Sources</i>	10
3.1.1	<i>Unique UNIT ID</i>	10
3.1.2	<i>Unique Recording FILE NUMBER</i>	10
3.1.3	<i>TIMING Sequence</i>	11
3.1.4	<i>CHECKSUM Errors</i>	11
3.1.5	<i>Other Errors</i>	11
4	<i>Irregularities</i>	12
4.1	<i>What are Irregularities</i>	12
4.2	<i>How Can Irregularities Occur</i>	12
4.3	<i>Tampering</i>	13
4.4	<i>When Irregularities Occur</i>	13
5	<i>Expert Witness</i>	14

Figures

Figure 1, <i>Authenticate Main Window</i>	4
Figure 2, <i>About Window</i>	4
Figure 3, <i>Authenticate Main Window</i>	5
Figure 4, <i>File Details Window</i>	6
Figure 5, <i>Progress Bar</i>	9
Figure 6, <i>Example with Irregularities</i>	9

1 Authenticate Software

The *Authenticate* software package is used to authenticate the information contained in downloaded *.IMG and *.IM2 audio files created from covert solid state surveillance recorders.

Unlike normal audio files which can be modified and resaved, these audio files have inherent features built in to guard against tampering.

1.1 Computer Hardware Requirements

The recommended minimum requirements for running *Authenticate* are,

- Pentium III 500MHz CPU
- 128MB of RAM
- Windows™ 98 operating system or later
- Sound card

1.2 Installing *Authenticate*

To install the *Authenticate* software onto Windows™ NT, 2000 or XP Operating Systems, you must log on to the computer with **Administrator** privileges.

Insert the *Authenticate* CD media into your computer.

The installation should auto-start. If not, it can be manually started by selecting **Run** in the Windows™ **Start** menu or by double clicking the ***Authenticate_setup.exe*** icon from the CD in **Windows Explorer**.

Follow the prompts until installation is complete.

2 Running Authenticate

Use the Windows™ **Start** menu or the desktop icon to run *Authenticate*.

2.1 *Authenticate* Main Window

Authenticate will display the following screen on start-up.

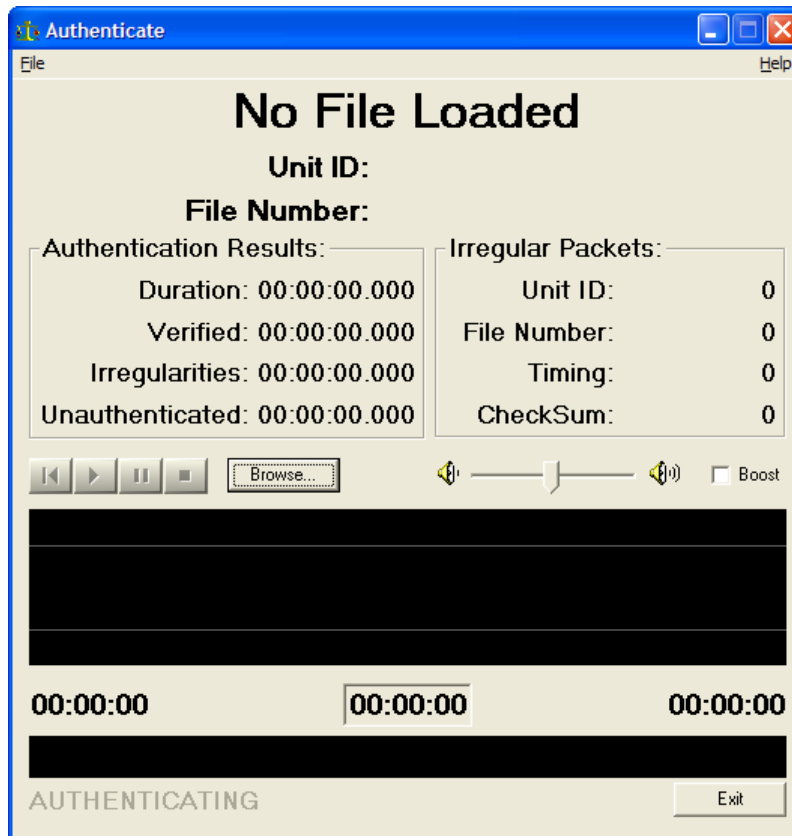


Figure 1, *Authenticate* Main Window

Buttons and menu items not currently available are grayed out until such time that they can be used.

2.2 *Authenticate* Version

To view the version of *Authenticate*, select About from the Help menu.

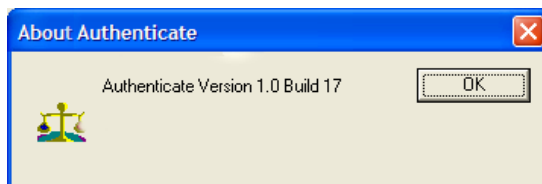



Figure 2, *About* Window



2.3 Loading Audio Files

Files can be loaded via two methods, the  button on the main window or from the File menu.

Either method will popup the standard Windows™ file browser and prompt you to find the *.IM2 or *.IMG file to be loaded.

Select the desired file and load it into the *Authenticate* program. Once a file is loaded the main window should take on an appearance similar to the example following.

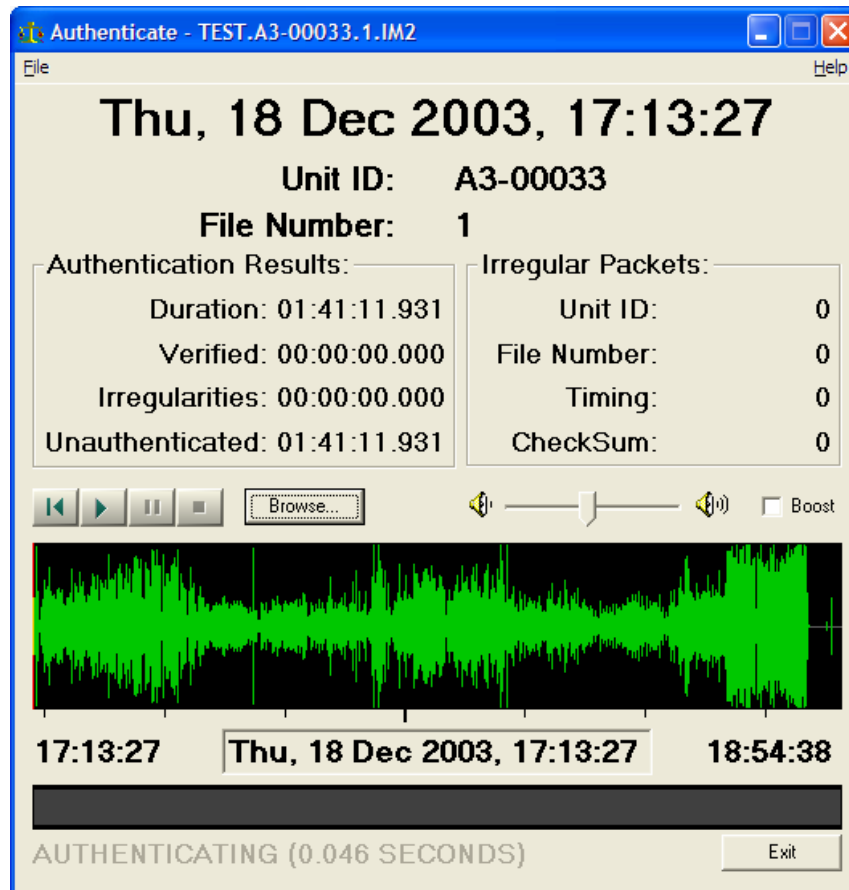
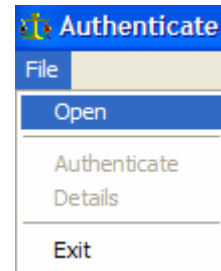


Figure 3, Authenticate Main Window

To provide maximum data integrity the *.IMG and *.IM2 formats include a proprietary structure which intertwines core recording information into a packet format. This means that each of the packets "knows" what recording it is part of and which recorder made it.

2.3.1 Audio File Details

To view the recording settings used on the audio file, select Details from the File menu.

The following window that will appear giving you the details on the settings used on the recorder for the loaded audio image file.

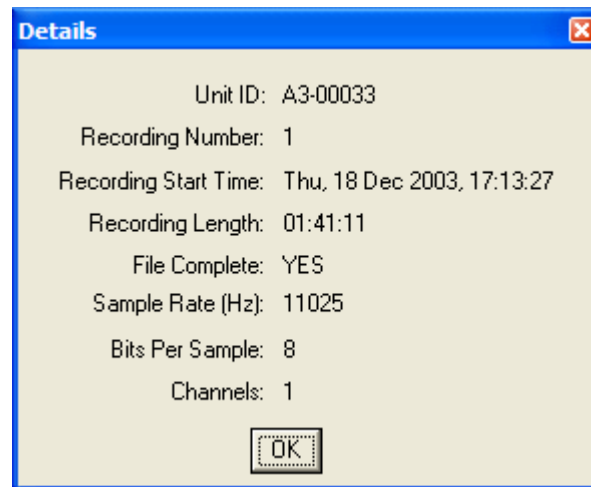
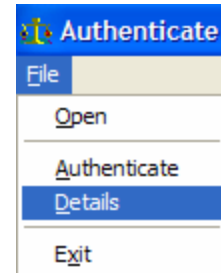


Figure 4, File Details Window

Property	Description
Unit ID	Displays the unique number of the recorder used to create the loaded audio file
Recording Number	Displays the unique recording number of the loaded audio file for that recorder
Recording Start Time	If available, this shows the time and date that recording commenced based on the internal clock of the recorder. Note: NA is the expected display for some models of recorders and does not indicate integrity loss. NA: displayed if the recorder did not support this feature
Recording Length	Displays the length of the loaded audio image file, displayed in hours, minutes and seconds format (HH:MM:SS).
File Complete	Is the recording complete Note: NA is the expected display for some models of recorders and does not indicate integrity loss. YES: the file is complete NO: the file is incomplete (data may be missing) NA: displayed if the recorder did not support this feature
Sample Rate (Hz)	The sampling rate used to record the audio image file, displayed in Hertz (Hz) – equivalent to samples per second.
Bits Per Sample	The number of data bits used to store each channel of each sample in the audio image file.
Channels	The number of channels used to record the audio image file. 1: Mono recording 2: Stereo or two channel recording

2.4 Main Window Descriptions

The following items of the main window are updated as each packet is processed and played back. The packet size displayed in seconds **AUTHENTICATING (0.046 SECONDS)** is shown on the bottom left of the window.

2.4.1 Current Packet Information

Thu, 18 Dec 2003, 17:13:27 Unit ID: A3-00033 File Number: 1	
Property	Description
Date and Time	Displays either the current date and time or the time since the recording commenced – depending on the recorder model used.
Unit ID	Displays the unique serial number for the unit on which the recording was made.
File Number	Displays the unique file number of the recording for that recorder.

2.4.2 Summary of Authentication Results

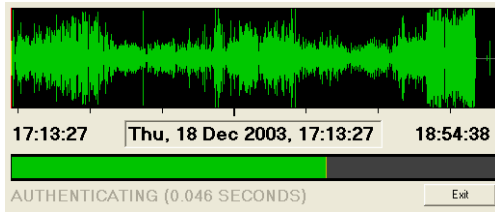
Authentication Results: Duration: 01:41:11.931 Verified: 01:05:54.885 Irregularities: 00:00:00.000 Unauthenticated: 00:35:17.046	
Property	Description
Duration	Displays the total length of the recording.
Verified	Displays the length of the recording that has been correctly verified.
Irregularities	Displays the length of the recording that has failed verification.
Unauthenticated	Displays the length of the recording that is yet to be verified.

2.4.3 Summary of the Most Common Irregularities

Irregular Packets: Unit ID: 0 File Number: 0 Timing: 0 Checksum: 0	
Property	Description
Unit ID	Displays the total number of packets that contain the incorrect unique serial number of the recorder.
File Number	Displays the total number of packets that contain the incorrect unique recording number for the recorder.
Timing	Displays the total number of packets that contain incorrect timing information.
Checksum	Displays the total number of packets that contain incorrect checksums.

Note: This is not a complete list of possible irregularities. All irregularities whether displayed here or not will be accounted for in the previous section 2.4.2 Summary of Authentication Results.

2.4.4 Waveform and Authentication Processing Information



Property	Description
Waveform	Displays a graphical view of the recorded waveform.
17:13:27	Displays either the start time for the recording or 00:00:00 depending on the model of the recorder used.
Date and Time	Displays either the current time of the recording or the time since the start of the recording – depending on the model of recorder used.
18:54:38	Displays either the end time or length of the recording depending on the model of recorder used.
Graphic Display Bar	Graphically displays the history of the verification process. Gray: yet to be verified Yellow: partially verified Green: correctly verified Red: incorrectly verified
Authenticating	Indicates the length of each verifiable packet, and flashes if authentication is in the process
Exit	Button to Exit program.

2.4.5 Replay Controls



Property	Description
Start Button	Moves the cursor to the start of audio image file.
Play Button	Plays back the loaded file through the computers sound card for listening.
Pause Button	Pause the playback of the recording.
Stop Button	Stops the playback of the recording.
Browse Button	Used for selecting a new recording to open for authenticating.
Volume Slider	Increase / decrease the playback volume
Boost	Check the box to amplify the playback volume.




2.5 Authenticating Audio Files

As each packet is played it is automatically authenticated and the window updated. Packets correctly verified make the bottom left text flash green **AUTHENTICATING (0.092 SECONDS)** whilst packets that are unable to be correctly verified will show display red **AUTHENTICATING (0.092 SECONDS)**.

The graphic display at the bottom of the window will give a visual history of the process where blocks are displayed as gray, yellow, green or red depending on whether they are unverified, partially verified, correctly verified or incorrectly verified.



Incorrectly verified blocks will always produce a red area on the graphic display no matter how small the packet as compared to the full file size.

The user is free to skip backwards and forwards by clicking into the audio sample window and by using the play  pause  and stop  buttons to control the replay and verification process.

At any time a loaded audio image file can be fully authenticated by selecting the Authenticate option from the File menu. A progress bar is displayed to indicate the state of processing.

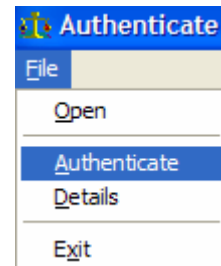
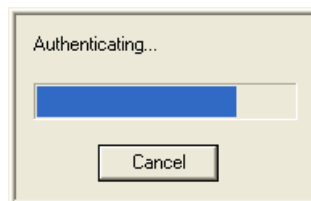


Figure 5, Progress Bar

The main window is also continually updated to show the status of the authentication process. An example of the main window for a file containing irregularities is shown below.

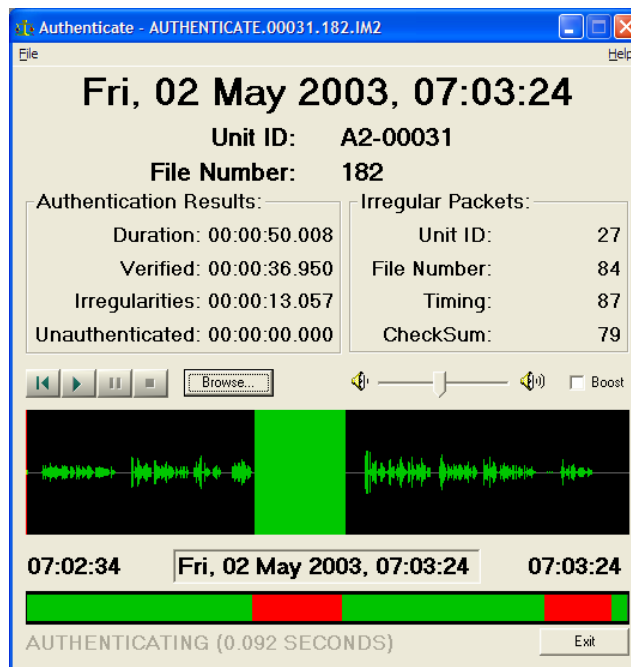


Figure 6, Example with Irregularities

The strength of the authentication process is that it shows exactly how much data is in doubt and exactly where the irregularities are in the audio image file. This ensures that even when irregularities occur the remaining data can be trusted and proven correct.

3 File Integrity

To ensure the validity of the recorded data sets and to safeguard continuity of evidence, the *.IMG and *.IM2 audio files use a packet data format that intertwines the recorded data with extra information so that data verification and integrity checking is possible. Packets are totally self-contained to prevent unauthorized changes of audio image file. The data is further protected by the proprietary nature of the format and by data encryption for some models of the recorders.

The size of each packet capable of being verified is displayed as the audio image file is authenticated and will generally represent between 0.005 and 0.15 seconds depending on the configuration and model of recorder.

3.1 Integrity Sources

An explanation of some the major integrity sources incorporated into each and every packet of the audio image file follows. Any failure to correctly verify a single packet will result in the changes to the 2.4.2 Summary of Authentication Results and 2.4.3 Summary of the Most Common Irregularities.

3.1.1 Unique UNIT ID

Each recording device is given a unique UNIT ID at the time of manufacture. The UNIT ID is coded into the internal memory of the unit and cannot be changed by the user.

The UNIT ID ensures audio image files from two or more different recorders have not been combined to create a new audio image file.

As the file is played the displayed unit id **Unit ID: A3-00033** would change.

Irregularities are coded red in the graphic display and summaries updated.

3.1.2 Unique Recording FILE NUMBER

Every recording made on a particular recording device, is given a unique FILE NUMBER. The FILE NUMBER is generated by the recording device and cannot be nominated by the user.

The FILE NUMBER ensures audio image files from two or more different recordings have not been combined to create a new audio image file.

As the file is played the displayed file number **File Number: 1** would change.

Irregularities are coded red in the graphic display and summaries updated.

3.1.3 TIMING Sequence

Each packet of audio data knows its position with the audio image file. The TIMING sequence is internally generated by the device and cannot be changed.

The TIMING sequence ensures sections of audio are not moved from their original position within the audio image file. On some recorders the timing sequence can be related back to recorders internal real time clock, on others it represents the elapsed time.

As the file is played the current time **Thu, 18 Dec 2003, 17:13:27** or the elapsed time from the start of file **Elapsed Time: 00:13:27** (depending on the type of recorder used) would appear to jump backwards and forwards or not change smoothly.

Irregularities are coded red in the graphic display and summaries updated.

***Note:** the current time if available is based on the recorders real-time clock as set by the user. Integrity is performed on the sequence of the timing not upon the absolute value. Failure to correctly set the devices real-time clock will not affect the integrity of the audio image file.*

3.1.4 CHECKSUM Errors

Each individual byte of audio data stored in the image file packet is manipulated to produce a CHECKSUM for the complete packet. At the time of verification a newly calculated CHECKSUM is compared to the CHECKSUM created at the time of recording to verify the complete data packet.

The CHECKSUM ensures each byte of audio data stored has not changed since the time of recording.

Irregularities are coded red in the graphic display and summaries updated.

3.1.5 Other Errors

Throughout the authentication process the recording parameters including sample rate, number of bits per sample and number of channels are continually checked.

Irregularities are coded red in the graphic display and summaries updated.

4 Irregularities

Irregularities within recordings are expected from time to time.

With analogue recordings we are used to hearing a small amount of static, hissing or the occasional click or pop in the replayed audio. These are all evidence of irregularities, the difference with a digital product is that any such irregularities can be exactly quantified and are therefore brought to our attention.

If irregularities do occur in a file being authenticated, they should be assessed with a view to determining how much data is in question, where in the file has the irregularity occurred, and what relevance does that section of data in question have to the audio file as a whole.

4.1 What are Irregularities

Most people have experienced a CD which skips during playback or a computer disk which contains errors, both of these are good examples of what might happen to an *.IMG or *.IM2 file from time to time.

Irregularities are pieces of data that are corrupt or otherwise damaged and cannot be validated by the authentication process. They are not necessarily wrong, they just cannot be verified as correct. Irregularities can be short, possibly less than a 10th of a second, or last for several minutes and will cause the audio to be unusable during that section of the file. Unusable audio will sound like loud static, or possibly silence.

Irregularities will show up as a red patch in the graphic display bar and will be listed in the **2.4.2 Summary of Authentication Results** and possibly the **2.4.3 Summary of the Most Common Irregularities**.

Irregularities in one section of a file have no influence on the other parts of an audio file.

4.2 How Can Irregularities Occur

There are three main areas where irregularities can occur, being, during recording, during transfer and during storage.

Some reasons for the failure include,

- Interference from other electronic devices, such as cell phones or radio transmitters.
- Power fluctuations to the unit.
- Physical influences such as shock or pressure.
- Minor electronic failures.
- Computer glitches during transfer.
- Damage to the storage medium.

Note: This is not a complete list.

4.3 Tampering

Most people with a computer could, with a little help or training, cut and paste an audio file to change it from the original. There may be a perception held by people that the same be true for *.IMG & *.IM2 files. This is not the case.

*.IMG & *.IM2 files are specifically designed to stop such interventions. When authenticated, tampering would be evident by large section of audio showing up as RED and containing irregularities in,

- **3.1.1 Unique UNIT ID**
- **3.1.2 Unique Recording FILE NUMBER**

or

- **3.1.3 TIMING Sequence**

Reverse engineering the packets and modifying the identifiers themselves is stifled by the chosen file format as explained in **3 File Integrity**.

4.4 When Irregularities Occur

If irregularities do occur then their effect on the integrity of the audio product should be assessed by ascertaining the length of the unusable section. Its position in the file, and it's influence on the remainder of the audio.

Once again, the file format chosen is specifically designed so that irregularities in one section of a file have no influence on the other parts of an audio file.

5 Expert Witness

For more information regarding the legal ramifications of presenting digital audio data in a court of law please contact a recognized expert in that field.

Paul Ginsberg of Professional Audio Laboratories is one such expert and has written many papers on the subject including, "*The Legality of Digitally Recorded Tapes*" which has particular relevance to this equipment. Paul can be contacted via,

Paul Ginsburg
President

Professional Audio Laboratories, Inc.
7 Skylark Drive
Spring Valley, NY 10977
United States of America

Telephone: (845) 354-2229
Fax: (845) 354-9222
Website: www.proaudiolabs.com
E-mail: engineeroo@aol.com