Contents

How to Setup Forensic Notes to Document Your Investigations ...................................................... 2

Creating Folders .................................................................................................................................. 3
  Deleting a Folder ............................................................................................................................... 6
  Creating Nested Folders ................................................................................................................... 8

Notetaking: Intake Officer .................................................................................................................... 9
  Creating a Notebook ........................................................................................................................ 9
  Creating the First Note .................................................................................................................... 11
  Adding Attachments .......................................................................................................................... 12
  Date & Time ...................................................................................................................................... 15
  Exhibit continuity / Chain of custody .............................................................................................. 16
  Note Date & Time vs. Timestamp Date & Time .................................................................................. 17

Notetaking: Forensic Examiner ........................................................................................................... 18

Creating Multiple Notebooks ............................................................................................................ 18

Forensic Examination – Exhibit #1 .................................................................................................... 20

Adding Images .................................................................................................................................... 20

Adding Emails ..................................................................................................................................... 25

Adding Tags ....................................................................................................................................... 26

Searching ............................................................................................................................................ 27

Continuing The Investigation ............................................................................................................. 28

Downloading a Notebook ................................................................................................................... 29

Further Questions ............................................................................................................................... 30
How to Setup Forensic Notes to Document Your Investigations

Forensic Notes makes it easy to setup and organize your notes for investigations, whether working as an individual or as part of a team.

The following information will allow you to familiarize yourself with the Forensic Notes application, including many new features for organizing & sharing notes in a team environment. Though investigations have typically been a team effort, investigators’ notes have typically not been easy to share, as they usually resided in a paper notebook. With Forensic Notes, you will now be able to easily share important information, without having to photocopy or somehow recreate key information. This increases collaboration and saves everyone a significant amount of time.

To assist you, it is highly recommended that you review the following Forensic Notes guides prior to setting up your Team Account.

1. **Getting Started Guide**: for a quick overview on how Sign-in to Forensic Notes, as well as the types of Notebooks available and how to create your first notes
2. **FAQ for Team Accounts**: for a quick overview on how to add team members

In this guide we will use a fictional digital forensics team that consists of two members who both will be using Forensic Notes to make contemporaneous notes during their investigations.

Det. Smith:

- "Administrator" of the Forensic Notes team account
- Uses Forensic Notes to:
  - Document the intake of exhibits (exhibit continuity / chain of custody)
  - Document the assignment of files to investigators
Det. Brown:

- “Member” of the Forensic Notes team account
- Uses Forensic Notes to:
  - Document taking possession of the exhibits (exhibit continuity / chain of custody)
  - Document his digital forensic examinations

Creating Folders
Forensic Notes allows you to create folders to help organize your investigations and digital notebooks. Notebooks can easily be dragged and dropped into different folders without affecting the content within the notebooks.

Moving Physical Paper Notebooks
This feature is similar to moving physical paper notebooks into different storage boxes or shelves as required.

Creating & Moving Folders
Only an Administrator can create and move folders within a Team Account. This ensures that the integrity and organization of your folder structures remains consistent throughout your organization.

Folders can also be moved, deleted, and nested into other folders by the Administrator(s).

In our example, Det. Smith and Det. Brown have just begun using Forensic Notes.

Det. Smith (Administrator) is going to setup the folder structure for managing the notes for her team’s investigations.

She has decided to have all notebooks organized by investigation file numbers followed by a brief description of the offence that is being investigated. To begin, she will create three new folders.
Steps Required:

1. Click on **down arrow** next to New in the “All Notebooks” panel.
2. Click **New Folder**.

NOTE: Repeat the above process for each new folder you wish to create. In our example, Det. Smith has created three (3) folders.

When completed her Team’s folder structure will look like the following:

---

**Creating Folders**

Each time you create a new folder, it will create (or nest) it within the selected node, depending on whether the folder or the root (“Group Account”) node has been selected.
If you accidentally create a folder in the wrong location, such as nesting a folder inside another folder, you can simply:

1. Drag & drop the folder to a new location (Desktop Only).

Folders are not very useful without names. To help you organize your team’s work, we suggest you rename each folder with an appropriate name.

To rename a folder you can either:

1. Double click on the folder name, which by default is (New Folder).

   OR

2. Click on the folder name in the editor pane.
3. After you have renamed your folder you must press ‘Enter’ to save the name change. (If you click somewhere else on the screen, the changes will not take effect).
I

n our example, Det. Smith will use the following folder name structure:

- <File Number> - <Type of Offence>

Deleting a Folder
At some point you may want to delete a folder or notebook. This is possible, if it does NOT contain a Timestamped Note.

Naming Folders

We recommend you name your folders in a way that is meaningful to you and your team. Each folder should have a unique name to identify the investigation. This will allow you to identify the correct notebook as the number of notebooks increase.
Deleting Notebooks

If a folder or notebook contains a Timestamped note, it cannot be deleted. Forensic Notes prevents deletion to help protect individuals and organizations from accusations that important documentation was destroyed, accidentally or intentionally.

If you need to delete a Notebook for legal reasons, please contact us at Support@ForensicNotes.com to discuss options.

To demonstrate the deletion of a Forensic Notebook with no Timestamped notes (known as Forensic Notes), Det. Smith will delete the auto-generated notebook which is created upon account creation within the root node.

Default Notebook

When you first create an account with Forensic Notes, your first notebook is automatically created. You are not obligated to use this Notebook and can either use it, or simply delete it.

To delete a notebook (or a folder):

1. Select the Notebook by clicking it
2. Click the trash icon at the top of the All Notebooks Panel
3. A pop-up box will appear to confirm if you want to delete the Notebook. Click Ok to delete.
4. You will then receive a confirmation message regarding the deletion.

Creating Nested Folders
Det. Smith now wants to begin organizing the folders for the Robbery file that the team will begin working on. To do this, Det. Smith selects the Robbery Folder and creates two new folders; one for each team member.

Det. Smith will name the folders with each of their names and their role in relation to the investigation.
Each investigator will now be able to create their own notebooks within their designated folders.

**Notetaking: Intake Officer**

Det. Smith is now going to create a Notebook in her folder to document all her actions involved with this Robbery Investigation.

**Naming Notebooks**

Everyone on your team should follow an agreed naming convention when creating new notebooks.

One method would be using: `<File Number>` - `<Your Name>` - `<Your Involvement>`


**Creating a Notebook**

1. Select the folder you want to create the Notebook in
2. Click the **down arrow** to create a new notebook
3. Select the type of notebook you want to use.

*(We recommend Forensic Notebook w/edits, for most users).*
Det. Smith then re-named the notebook in the exact same manner as renaming a folder (discussed above).

Det. Smith can now begin taking contemporaneous notes for this investigation.
Creating the First Note

**Contemporaneous Notes Required!**

Digital Forensic Organizational Bodies agree that you MUST create Contemporaneous Notes as part of all Digital Forensic and Open-Source investigations.

For further information, refer to our [Digital Forensic Documentation](https://www.ForensicNotes.com) article.

Chain-of-custody is yet another area that must be fully documented to ensure you and your organization can always account for where an exhibit was once it comes into your custody. When Det. Jones from the Robbery Unit arrives with exhibits, Det. Smith begins to document receipt of the exhibit by clicking “New” in the Selected Notebook panel to begin her first note.

**Naming Notes**

Det. Smith will name her first note “Intake of Exhibits”.

![Image showing the process of creating a new note and naming it](image-url)
Det. Smith now begins to take notes regarding the intake of the exhibits by clicking into the editor box. This will cause the popup toolbar to be displayed allowing you to format your notes as needed.

**Adding Attachments**
Forensic Notes not only allows Det. Smith to take contemporaneous notes about important documentation she has received, but also attach documents related to the investigation such as:

- Warrants
- Consent Forms
- Work Submission Forms

Det. Smith decides she will attach both the internal work submission form and the warrant authorizing the search of the exhibits.

**Naming Notes**

Renaming a note is completed in the same manner as renaming a folder or Notebook which was discussed above.

**Naming individual notes is NOT necessary**, but it can be helpful later when trying to locate specific information.

* Note Names are searchable with the Forensic Notes search function; whereas the content of your notes is not. Therefore, coming up with standardized note names can be useful for finding information later in your investigation.

**NOTE**: Note names do NOT appear within any Notebook PDF’s generated. They are only visible within the Forensic Notes application.
Adding Attachments

Adding Attachments in Forensic Notes receive the same Digital Signing & Timestamping benefit as the notes you create. This feature helps increase the authenticity & reliability of any documents you received, showing they were not altered at a later time.

In fact, we encourage users to attach copies of all relevant documentation, images, and even videos, to ensure these types of files can also benefit the power of Forensic Notes. Forensic Notes doesn’t compress your files, (including images & videos) to ensure you always have an exact copy.

Lastly, attaching files ensures they are easy to locate and won’t be lost or misplaced.

To add an attachment, you can either:

- Drag & drop
- Or click within the Choose a file box

You can click ‘Choose a file’ or drag files to attach them to your notes.

Received from Lead Investigator Det. JONES three exhibits, numbered: Exhibit #1, #2, #3.
- Examinations are requested in relation to robbery investigation.
- Each exhibit was in a sealed RF shielded can.
- Confirmed warrants and submission forms present to proceed with forensic examination (and attached w/ notes).
Confirming Attachments are Properly Uploaded

Before Timestamping or viewing a different note, confirm that your attachment(s) are properly uploaded by ensuring that it displays 100% upload.
Date & Time

Notice that Det. Smith has not made note of the date and time she received the Exhibits. She doesn’t need to record the time, as it’s automatically recorded when the note was created.

Date & Time are automatically added when creating a note.
You can change the date / time by clicking inside the box.

Date & Time

Each time you create a note, the Date & Time are pre-filled at the time the note was created. This Date & Time box is a useful for recording the time you did an activity, and is completely independent of the Timestamp.

Under most circumstances, the Timestamp time will be relatively close to the time of the note. However, if you have a need to backdate a note to show when you completed a task, you can without affecting your credibility as the Timestamp time will properly show when the note was locked from further edits.
Once Det. Smith has attached her documents and recorded the relevant information she can then Timestamp her note, proving the contemporaneity of when the note was entered.

To do this, she simply clicks the blue Timestamp button at the bottom of the note editor. This will finalize the note, which Digitally Signs and Timestamps it, generating a Forensic Note. This Forensic Note can then be verified if required in the future.

Exhibit continuity / Chain of custody

Det. Smith continues to add new notes to document her administrative tasks. Next, she records the time she placed the exhibits into a secure locker before timestamping the note.

### Backdating Notes

If you need to ‘backdate’ a note to show when you performed a task, then it is recommended that you add an extra note explaining why the Timestamp for the note is hours or days after the date/time of the note.

As with most legal issues, you will not run into issues if you can properly explain and articulate the reasons for an issue brought up by the opposing party.

### Modifying Timestamped Notes

If you are using a “Forensic Notebook (w/ edits)”, you can “edit” existing Timestamped notes which will allow you to create new versions of a note.

The original Timestamped note will be included within the Forensic Notebook allowing for full-disclosure.

For further information, refer to our [Types of Notebooks](#) page.
Approximately three hours later, Det. Smith documents when she transferred the exhibits to the digital examiner by creating a new contemporaneous note to record this activity.

Note Date & Time vs. Timestamp Date & Time

Once you Timestamp a note, you will notice that each note will have two (2) different Date/Times associated.

1. Date & Time (set by user)
2. Date & Time (set by Timestamp)

This ensures that you are able to easily articulate when the action occurred in comparison to when you Timestamped the note dis-allowing any future edits.
Det. Smith has now completed the intake process and plans to transfer all exhibits to Det. Brown. Det. Brown will also use Forensic Notes to document his actions during the forensic examination.

**Notetaking: Forensic Examiner**

**Creating Multiple Notebooks**

When Det. Brown (Examiner) now accesses his Forensic Notes account, he will see all the folders and notes that Det. Smith created.

Det. Brown decides to create an “Overview” Notebook. This “Overview” Notebook will be used to document all actions associated with the investigation, but not specific examination steps for an individual exhibit.

He will then create a unique notebook for each exhibit he will examine.

Creating a separate Forensic Notebook will help to keep the notes organized, searchable, and simplify the disclosure process.
In the “Overview” Notebook, Det. Brown records notes regarding the date and time he received the exhibits (ensuring Exhibit Continuity) and receiving essential documents such as the Work Request Form and a copy of any Warrants authorizing the digital forensic search.

He also records information related to the investigation, such as direction provided from the lead investigator, as shown below.
Forensic Examination – Exhibit #1

After recording key information into the “Overview” Notebook, Det. Brown begins work on his first exhibit. As a result, he creates his first note in the “Exhibit #1 – iPhone (white)” Forensic Notebook.

Det. Brown names his first note, “Initial Examination”.

Det. Brown not only documents the initial steps during the forensic examination, but he also adds a photo of the exhibit to aid his documentation.

Adding Images

Det. Brown could add the image as an attachment; much like Det. Smith did with the forms and warrant. However, Det. Brown wants to easily view this image within the note itself.

To add an image into a note:

- Simply drag and drop the photo directly into the note.
- Once an image is in a note, it is easy to move and re-adjust its size.
Embedded Images in Notes

Forensic Notes doesn’t compress images that are embedded into your notes – even if resized within the editor to make it fit better within your notes.

This has two benefits:

1) Image quality is never lost – which can especially be important when dealing with potential evidence.
2) The original image is saved as an external image which can be downloaded and printed in full size, if required, for evidentiary or disclosure purposes.

For Open-Source investigations (OSINT), this is especially important as you capture evidence on the web which you may later find to be key evidence in your case.
Det. Brown continues to work on the phone throughout the day, and breaks his notes up to identify various activities throughout the forensic process (as shown below).

This process of breaking down the notes into various sections can make it easier for himself or other team members to locate information at a later date if needed.
While Det. Brown was verifying the data extraction, he came across an important conversation within his favorite mobile forensic software. The text message stated “This time don’t shoot anyone”.

He makes a careful note of the discovery within his notes and also takes a photo of the visible conversation on the exhibit to clearly show where the message should be appearing if it hadn’t been deleted.

Using 3rd party photo editing software, he adds comments onto the image prior to dragging it into the Forensic Notes application.
Editing Images within Forensic Notes

You can edit images within Forensic Notes adding text, handwritten remarks and arrows to highlight key findings within images.

Mobile Devices

To add an image as displayed above using a mobile device, you could:

1) Click the “Insert Image” icon
2) Select to take a picture (or select existing image on phone)
3) Add image and click “edit”
4) Add text and handwritten remarks as needed.
Adding Emails
Det. Brown sent off a preliminary report to the lead investigator requesting he review the report and advise what relevant information to include in a final Digital Forensic Report.

The lead investigator responded by email identifying what was relevant later in the day.

Instead of just making a note that that he received an email that identified relevant information, Det. Brown saves the email as a PDF and then attaches it directly to the note. This ensures that all the information is located together as well as digitally signed and timestamped.

Attachments
Remember, almost any file type can be attached to Forensic Notes. Attaching files helps to keep all relevant information within your notes. It also ensures that all your documents benefit from timestamping and digital signing – ensuring you can prove the files weren’t altered at a later date.
Adding Tags

As Det. Brown continues to use Forensic Notes, he will eventually have hundreds of notes documenting all the examinations he has conducted. As time passes, he may forget whether he received an email about this exhibit. Therefore, to help with locating key information, he takes advantage of the Tagging feature.

In particular Det. Brown likes to be able to search for “email” and “report”, in the event he forgets whether he contacted anyone about this file and the report by email. By doing so, he can use the search feature to quickly find the related note(s).

To add a new Tag into the “Tags” list:

1. Click into the “Tags” list bar and type the word you would like to add
2. Once a Tag has been added to your “Tags” list, anytime you use that word within your notes, the tag will automatically be selected and searchable
3. Underlined words within your notes indicate that they are part of your “Tags” list
4. To view a list of all available Tags, click within the “Tags” list bar. This will display a scrollable list of available Tags

Organizing Your Notes & Notebooks

This document contains just one way of organizing your notes. You may decide to further breakup your notes into additional Forensic Notebooks to make disclosure easier by being able to keep some notebooks from disclosure unless required.

As an example, you may decide that you want to document the above email conversation, but not necessarily within your examination notes as described above. In this case, you may decide to create a Forensic Notebook that only includes conversations with investigators. ThinkDFIR.com has a good article that discusses another structure for documentation to consider within Forensic Notes.
Searching

If Det. Brown wants to find his notes regarding the email he received from the lead investigator, he can quickly search and find those notes using the search bar located in the upper section of the Forensic Notes app.

The results will be displayed in a side menu that appears after initiating the search.

Tags

As a security measure, content of notes are not searchable, however tags can be created, which are searchable and very useful to help locate and find important information.

Tags can be manually added within the Tags section. Once a Tag has been entered, it will automatically get added each time that word appears in any future notes.

Forensic Notes contains a long list of default tags related to Digital Forensics and OSINT.

Search Tool – Desktop Only

Currently, the search is only available on Desktop versions of the application.
Continuing the Investigation
Det. Brown continues to use Forensic Notes to document all the exhibits related to this investigation.

After he is finished examining all the exhibits, you can see that the “Robbery” folder contains a total of five Forensic Notebooks, and each Forensic Notebook contains several Forensic Notes.
Downloading a Notebook
Lastly, at some point, Det. Brown may need to disclose these notes or decide to download a copy for review. Since he created a separate notebook for each exhibit, this will make disclosure simple and efficient ensuring that he does not have to redact information not related to the exhibits being used as evidence.

For example, if only Exhibit #1 is required for court, Det. Brown can quickly download just the notebook documenting activity related to Exhibit #1. The Notebook downloads as a password-protected ZIP Archive. The ZIP Archive will include:

- Forensic Notebook (PDF)
- Attachments
- Embedded Images
- Forensic Notes (individual Digitally Signed and Timestamped)
- Individual Timestamp certificates to assist with validation (if required)
Further Questions
If you have any further questions not answered by this guide or our FAQs, please contact support via email at support@forensicnotes.com.