Author Guide

Welcome to No Starch Press! Here's a brief guide to many of the practical details involved in creating a book with us. If your questions aren't covered here, please check with your editor or our production people and we'll do our best to answer them.

A Quick Who's Who

We're loosely divided into three teams: Editorial, Production, and Sales and Marketing. We say "loosely divided" because we sometimes overlap; our company is essentially one big team with various roles to play. You'll likely hear from most of us over the course of your project, but you'll also have a specific Acquisitions Editor, Production Editor, and marketing person assigned to your book.

You'll find our staff bios at *http://nostarch.com/about.htm*. Our email addresses are usually just our first names at *nostarch.com*, so we're easy to find.

Submitting Chapters

Please submit your manuscript as individual chapters, not as one big book, in Word or OpenOffice/LibreOffice format (unless agreed otherwise with your Acquisitions Editor). Embed all images in the chapter (low res is fine for editing purposes) so that we'll see a chapter complete with all elements.

Name your graphics in order of appearance (for example, *mybook01_01.png*, *mybook01_02.png*, and so on) and be prepared to send us all the image files for a chapter when it reaches the copyediting stage. We'll be importing your copy-edited chapters into a layout program, and we'll import your final images at that time. Add an insertion note in your manuscript for each image using the "Production Directive" paragraph style (for example, "insert <image filename>").

Styling Your Manuscript (Using Templates)

Please use the Word or OpenOffice/LibreOffice template included in this packet to style your manuscript. Attach the template to your document and then apply the paragraph styles and character styles to tell us how you want us to style your text.

- Paragraph styles style all text up to a hard return.
- Character styles style a word, phrase, or character differently from the rest of a paragraph.

The paragraph and character styles are mapped to the styles in the layout template we'll use for your book. This means that there's no need for you to "lay out" your manuscript. But it also means that any formatting you apply without a style may be lost when it's imported into the layout program. So if you want to make a word

italic, don't just click the *I* formatting button—use the *EmphasisItalic* character style. See page 8 for some examples of manuscripts and laid-out pages.

If you need help attaching or using the templates, see "How to Use Templates" on page 6. If you have existing work that is formatted but not styled, or if you have any questions about using styles, please contact your Production Editor. We're happy to help.

Styling Code

When styling your code, please apply styles as follows:

- Each line should be its own paragraph (ending with a hard return).
- Lines can be up to 78 characters long in standard layout; "wide" lines are 95 characters. If your lines will break, break them and indent the second line as appropriate.
- Use only spaces (not tabs) for whitespace and indents in code.
- Use **`LiteralBold`** for user input and highlighting; use ***`LiteralItal`*** for placeholders (such as ***`username`***); and use Wingdings (❶, ❷, ❸, ❹, ❺, ❻, ❼, ❽, ❾, ❿) to talk the reader through your code. (Your Aquisitions Editor can discuss this with you.)

What Kind of List Is It?

We use various list styles in our books.

Bullets A collection of points in no particular order

Numbers A step-by-step progression, such as a how-to

Plain Items or terms followed by descriptions (like this one!)

If you're associating two or more categories of items, you may be better off using a table rather than a list.

Images

Please discuss your planned images with us as early in the writing process as possible to make sure that they're in the right format and at the correct dpi. And of course, if you're using any images that you do not own, please be sure to request permission for them. (Your editor can supply you with a permissions form.)

Standard figure size on a finished book page is about 4.5 inches wide, so consider whether the important information in your image will be readable at that size.

Wherever you include images, be sure to "clear your visuals." That is, make sure that you reference your image in text before the image appears, and talk your reader through the visual. Make sure that they know what you want them to see in your image, and don't overwhelm them with stuff that's irrelevant. If you want to show your reader just a particular pop-up menu, consider showing only that menu or zoom in on the menu and crop out most of the background.

Screenshots

When capturing screenshots, please keep the following rules in mind:

- Use only the lossless PNG or TIFF file formats. Do not save as a JPEG or use JPEG compression in a TIFF file. This creates "noise" around high-contrast elements like text.
- Capture screenshots at your operating system's native dpi of either 72 or 96. Do not increase or decrease the resolution of your captured images.
- Keep cursors out of your screenshots unless you're using them to point something out. Stray cursors just look messy.
- Try not to include personal information, ads on websites, or other extraneous content that might confuse or distract your reader from your message.

Diagrams

When creating diagrams (whether finals or roughs for us to re-render), please do the following:

- Send us editable EPS, SVG, or AI files so we can make corrections during copyedit and proofreading.
- Your diagrams should read left to right, clockwise, or top to bottom.
- Use simple boxes, lines, or arrows for annotations and description. Keep things simple and clear, and don't get fancy unless fancy is the point.

Photographs

When producing and using photographs, please keep the following in mind:

- Take photos at the largest size available on your camera, and please do not resize them. A digital camera might give you a 72 dpi file at approximately 20×30 inches, which will size down to more than 300 dpi in layout.
- Save photos as JPEG, TIFF, or PNG.
- Please don't modify your images unless you've discussed doing so with your Production Editor. It's better for us to see your primary sources first so that we can advise as to the best way to handle them.
- When taking photos, try to avoid using complex backgrounds, and use soft lighting if possible.

Photography is an art, and we don't claim to be experts. You can find various tutorials online as well as suggestions for creating your own setups for photo shoots. We'll help and advise where we can, of course.

Illustrations

Illustrations should be vector files or hi res for clear printing. Please check with your editor about sizing, file types, and other details.

Color

Whether your book is one color (black and white) or four color, please consider the following when creating images:

- For *diagrams and other illustrations*, make sure meaningful colors or shades of gray are consistent and easily recognizable.
- For *screenshots*, avoid large areas of black where possible.
- For *photographs*, use good contrast, especially for important details. Aim for a good balance of dark areas, light areas, and midtones in black and white photos. In color photos, you'll probably want bright, vibrant colors.

Our Editing and Production Process

Please don't send us chapters until you think they're ready for editing, and send us only complete chapters (with images embedded), unless you've arranged differently with your editor. We're generally not in a rush. We want you to take the time to make your work great.

Once we've received your chapter, we'll edit using tracked changes and then send your chapter back to you to review. When reviewing, we suggest hiding the changes but still recording them. It's much easier to read a chapter without all of those messy revision marks. And be sure to use tracked changes when you make edits and revisions, so we can focus on the new material when you return the chapter to us.

Our editing and production process goes something like this:

1. You submit a chapter. Your editor reads and edits the chapter, focusing on structure and other high-level concerns.
2. You receive your edited chapter for review and revision, and return it to us.
3. We review your reworked chapter and may send it back to you again. If not, it's off to technical review.
4. The technical reviewer (an outside reviewer who's knowledgeable on the topic) reads the text, tests code and project how-tos, and so on. The tech review comments go back to you for any necessary fixes.
5. We tidy up the chapter and send it to Production. Next it goes to a copy-editor to clean up more granular details, line by line, with an eye toward consistency.
6. You receive the copyedit for review so you can revise as necessary and make sure that the copyeditor did not introduce any technical errors or misinterpret what you were trying to say.
7. You return the chapter to us and we move it into layout.
8. Laid out pages go to you for review and to proofreading. You and the proof-reader make sure that everything is laid out correctly, and the proofreader also checks for any remaining typos or inconsistencies.
9. We'll make corrections from your review and proofreading. At this point we will probably have some remaining queries for you, but the pages will be almost final.

10. Now we do another review to check corrections, and once the whole book catches up to this point, it's indexed (unless you've been indexing all along). Then it's off to the printer!

The most important thing to realize here is that you will have lots of opportunities to review and revise and tweak your chapters, so go ahead and send them to your editor! You'll get them back.

Indexing

Unless you've arranged otherwise with your editor, you are responsible for your index. This means that either you will create your index or we will hire a professional indexer on your behalf. Please be sure to discuss indexing with your editor early and decide what's best for you.

Creating an index is a significant amount of work, but a good author-made index is usually the best kind of index, because no one knows the content of the book better than you do. You can create your own index by tagging your manuscript files if you are using Word or a markup language like LaTeX. (In our experience OpenOffice/LibreOffice does not have reliable index tags; they tend to disappear.)

What Part of the Book Is This?

Some authors have been confused about what constitutes each part of a book. Here's a brief list. (Your book may or may not include all of these pieces.)

Dedication A few words or a line dedicating the book to a person or group.

Foreword A note by someone other than you telling readers about your book and, ideally, how great it is. The foreword should be written by an expert in the field and will typically run from two to four pages.

Preface Your discussion of the process of writing the book, including why you wrote it, how you researched it, and so on. A preface should run about two to four pages.

Contributors A page or two about the book's contributors, such as authors, technical reviewers, or illustrators.

Acknowledgments A thank-you from you to your friends and family, colleagues, editors, and so on. This might be one page or so unless you worked with several people. And if you did, thank them all. Each one of them becomes a champion for your book.

Introduction An introduction to the material in the book, with substantive information including a brief walkthrough of each chapter, an introduction to terms and conventions, installation instructions for software, or other things readers need to know before they start reading the rest of the book.

Chapter 1 The first chapter in your book should cover beginning material but with the same structure and length as the rest of the chapters in the book.

How to Use Templates

Here's how to apply templates in Word and OpenOffice/LibreOffice.

Applying nsp_au_template.dot in Word

You can open a new untitled document with the template attached by double-clicking the template file itself (*nsp_au_template.dot*). This file also contains examples and explanations of the styles we use.

In Word 2003 and Earlier

To apply the template to an existing document:

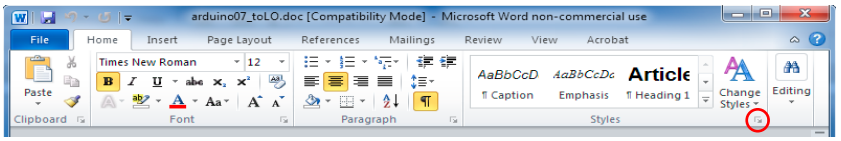
1. Open your chapter.
2. Go to **Tools ▸ Templates and Add-ins**.
3. Click the **Attach** button and browse to *nsp_au_template.dot*.
4. Check the box next to the words *Automatically update document styles*, and then click **OK**.
5. Go to **Format ▸ Styles and Formatting**. The Styles and Formatting pane should open at the right side of your document window. (The Styles and Formatting pane is available in Word 2002 and later versions.)
6. In the drop-down menu at the bottom of the Styles and Formatting pane, choose **Show: Formatting in use** or **Show: All Styles**. Apply No Starch Press styles as necessary by selecting text and clicking the styles in the Styles and Formatting pane. If the version of Word you're using doesn't offer this Styles and Formatting pane, you can also select and apply styles using the drop-down menu on the toolbar.

In Word 2007 or Word 2010

To apply the template to an existing document:

1. Open your chapter.
2. From the **Office Button** menu (2007) or the **File** tab menu (2010), choose **Word Options** or **Options**.
3. Choose **Add-Ins** from the left side of the Word Options dialog.
4. On the right side of the window, near the bottom, choose **Templates** from the **Manage** drop-down list. Click **Go**.
5. Click the **Attach** button and browse to *nsp_au_template.dot*. Click **Open**.
6. Check the box next to the words *Automatically update document styles*, and then click **OK**.

7. Navigate to the Home tab and click the small diagonal arrow at the bottom-right corner of the Styles gallery. The Styles pane will appear on the right side of your document.



Viewing Paragraph Styles

In Word 2003 and earlier versions, you can view paragraph style labels in the margin of your workspace by doing the following:

1. Select **View ▸ Normal**.
2. Go to **Tools ▸ Options**. Under the View tab, near the bottom, there is a setting called Style Area Width. In the measurement box, enter 1.0" (or more). A Style Area should appear to the left of your text, like a margin. The name of the paragraph style for each paragraph will be visible.

In Word 2007 or Word 2010, you can view paragraph style labels in the margin of your workspace by doing the following:

1. Navigate to the View tab and select the Draft view.
2. From the **Office Button** menu (2007) or the **File** tab menu (2010), choose **Word Options** or **Options**.
3. Choose **Advanced** from the left side of the Word Options dialog.
4. On the right side of the window, scroll down to Display. In the box next to the words *Style area pane width in Draft and Outline views*, enter 1.0" (or more). A Style Area should appear to the left of your text, like a margin. The name of the paragraph style for each paragraph will be visible.

Applying nsp_au_template.ott in OpenOffice/LibreOffice

You can open a new untitled document with the template attached by double-clicking the template file itself (*nsp_au_template.ott*). This file also contains examples and explanations of the styles we use.

To apply the template to an existing document:

1. Open OpenOffice/LibreOffice.
2. Press CTRL-O and navigate to and select *nsp_au_template.ott*. (The template is in OOo 2.x format.)

Style Area showing paragraph styles in Word

Character styles are shown in blue

Body
CodeA
CodeB
CodeB
CodeB
CodeB
CodeB
CodeB
CodeB
CodeB
CodeB
CodeB
CodeB
CodeB
CodeB
CodeC
Listing
Body

FakeDNS, we redirect the DNS request for *evil.malwar3.com* to our local host. Assuming that the malware is going out over port 80 (a common choice), we can use Netcat to listen for connections before executing the malware.

Malware frequently uses port 80 or 443 (HTTP or HTTPS traffic, respectively), because these ports are typically not blocked or monitored as outbound connections. Listing 3-2 shows an example.

```
C:\> nc -l -p 80 ❶
POST /cq/frame.htm HTTP/1.1
Host: www.google.com ❷
User-Agent: Mozilla/5.0 (Windows; Windows NT 5.1; TWFsd2FyZUh1bnRlcg==; rv:1.38)
Accept: text/html, application
Accept-Language: en-US, en:q=
Accept-Encoding: gzip, deflate
Keep-Alive: 300
Content-Type: application/x-form-urlencoded
Content-Length

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

Z:\Malware> ❸
```

Listing 3-2: Netcat example listening on port 80

The Netcat (nc) command ❶ shows the options required to listen on a port. The -l flag means listen, and -p (with a port number) specifies the port on which to listen. The malware connects to our Netcat listener because we're using FakeDNS for redirection. As you can see, *RShell* is a reverse shell ❸, but it does not immediately provide the shell. The network connection first appears as an HTTP

To use ApateDNS, set the IP address you want sent in DNS responses at ❷ and select the interface at ❹. Next, press the **Start Server** button; this will automatically start the DNS server and change the DNS settings to localhost. Next, run your malware and watch as DNS requests appear in the ApateDNS window. For example, in Figure 3-9, we redirect the DNS requests made by malware known as *RShell*. We see that the DNS information is requested for *evil.malwar3.com* and that request was made at 13:22:08 ❶.

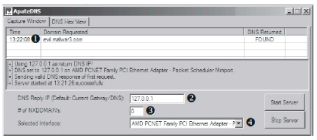


Figure 3-9: ApateDNS responding to a request for evil.malwar3.com

In the example shown in the figure, we redirect DNS requests to 127.0.0.1 (localhost), but you may want to change this address to point to something external, such as a fake web server running on a Linux virtual machine. Because the IP address will differ from that of your Windows malware analysis virtual machine, be sure to enter the appropriate IP address before starting the server. By default ApateDNS will use the current gateway or current DNS settings to insert into DNS responses.

You can catch additional domains used by a malware sample through the use of the nonexistent domain (NXDOMAIN) option at ❸. Malware will often loop through the different domains it has stored if the first or second domains are not found. Using this NXDOMAIN option can trick malware into giving you additional domains it has in its configuration.

Monitoring with Netcat

Netcat, the "TCP/IP Swiss Army knife," can be used over both inbound and outbound connections for port scanning, tunneling, proxying, port forwarding, and much more. In listen mode, Netcat acts as a server, while in connect mode it acts as a client. Netcat takes data from standard input for transmission over the network. All the data it receives is output to the screen via standard output.

Let's look at how you can use Netcat to analyze the malware *RShell* from Figure 3-9. Using ApateDNS, we redirect the DNS request for *evil.malwar3.com* to our local host. Assuming that the malware is going out over port 80 (a common choice), we can use Netcat to listen for connections before executing the malware.

Malware frequently uses port 80 or 443 (HTTP or HTTPS traffic, respectively), because these ports are typically not blocked or monitored as outbound connections. Listing 3-2 shows an example.


```
C:\> nc -l -p 80 ❶
POST /cq/frame.htm HTTP/1.1
Host: www.google.com ❷
User-Agent: Mozilla/5.0 (Windows; Windows NT 5.1; TWFsd2FyZUh1bnRlcg==;
rv:1.38)
Accept: text/html, application
Accept-Language: en-US, en:q=
Accept-Encoding: gzip, deflate
Keep-Alive: 300
Content-Type: application/x-form-urlencoded
Content-Length

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

Z:\Malware> ❸
```

Listing 3-2: Netcat example listening on port 80

The Netcat (nc) command ❶ shows the options required to listen on a port. The -l flag means listen, and -p (with a port number) specifies the port on which to listen. The malware connects to our Netcat listener because we're using ApateDNS for redirection. As you can see, *RShell* is a reverse shell ❸, but it does not immediately provide the shell. The network connection first appears as an HTTP `POST` request to `www.google.com` ❷, fake `POST` data that *RShell* probably inserts to obfuscate its reverse shell, because network analysts frequently look only at the start of a session.

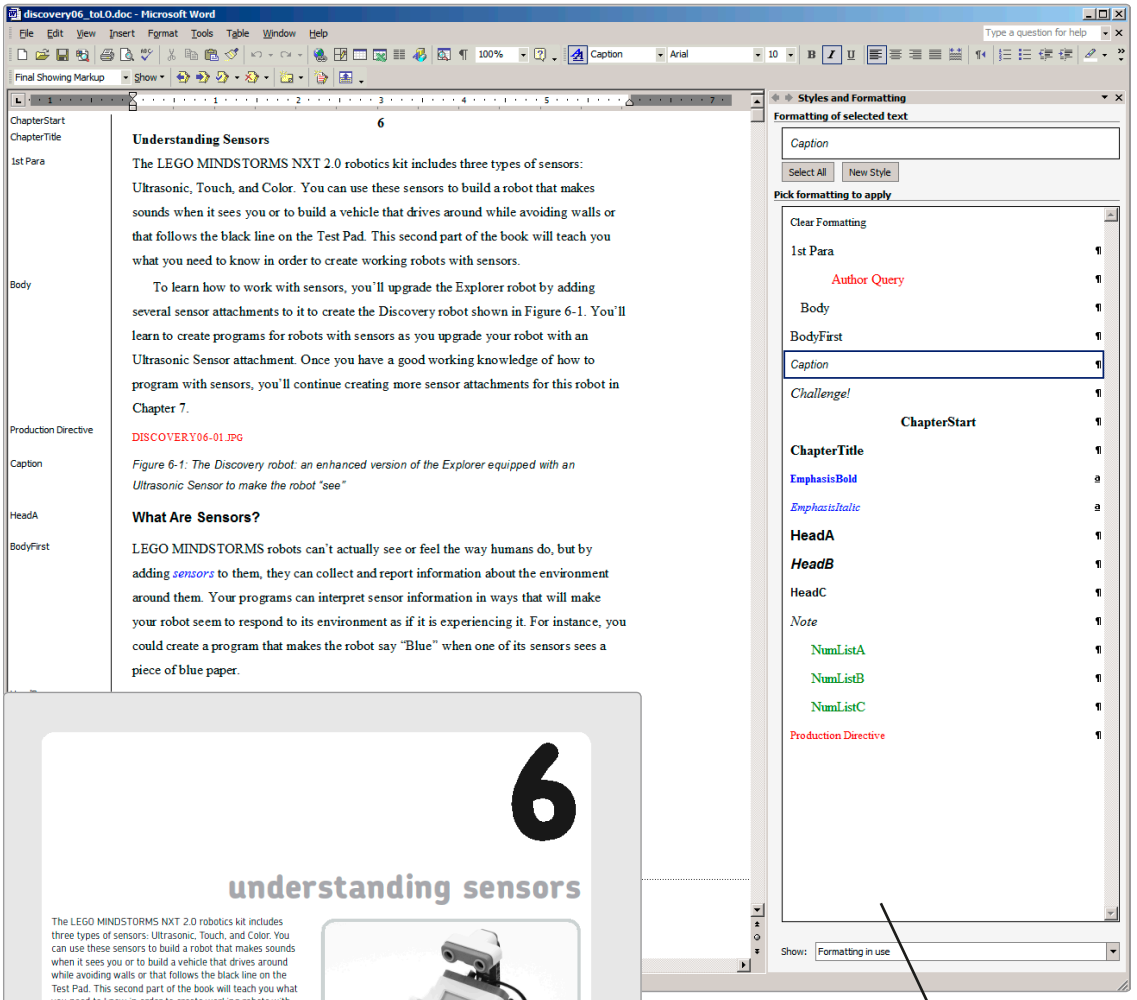
Packet Sniffing with Wireshark

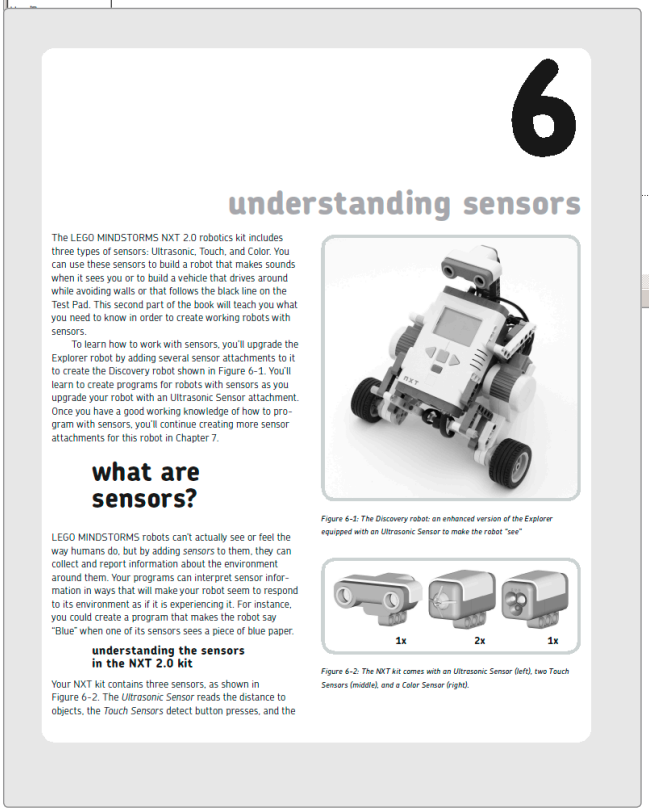
Wireshark is an *open source sniffer*, a packet capture tool that intercepts and logs network traffic. Wireshark provides visualization, packet-stream analysis, and in-depth analysis of individual packets.

Like many tools discussed in this book, Wireshark can be used for both good and evil. It can be used to analyze internal networks and network usage, debug application issues, and study protocols in action. But it can also be used to sniff passwords, reverse-engineer network protocols, steal sensitive information, and listen in on the online chatter at your local coffee shop.

The Wireshark display has four parts, as shown in Figure 3-10:

- The Filter box ❶ is used to filter the packets displayed.
- The packet listing ❷ shows all packets that satisfy the display filter.
- The packet detail window ❸ displays the contents of the currently selected packet (in this case, packet 47).
- The hex window ❹ displays the hex contents of the current packet. The hex window is linked with the packet detail window and will highlight any fields you select.

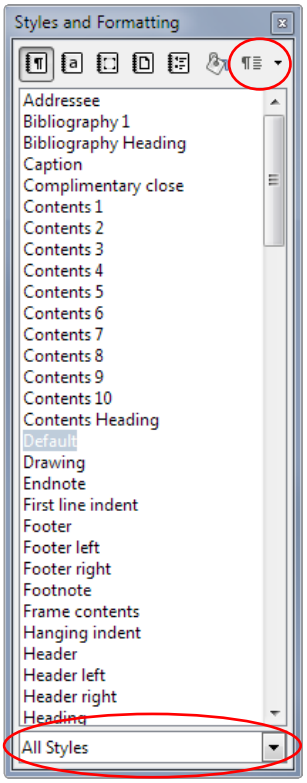




Word's Styles and Formatting pane showing formatting in use

Examples of manuscript pages in Word and the same content in layout (this page and facing page)

3. Choose **File ▸ Templates ▸ Save**. Type **`nsp_au_template.ott`** into the field at the top of the window. Make sure *My Templates* is highlighted, and then click **OK**.
4. Open your chapter.
5. Press F11 to open the Styles and Formatting window.
6. Click the button at the top right of the Styles and Formatting window, and select **Load Styles**. The Load Styles window should pop up (it is similar to the window you saw in step 3). Select *My Templates* and *nsp_au_template*, and then click **OK**.
7. Return to the Styles and Formatting window. Click the drop-down arrow at the very bottom and select **All Styles**. You should now see all the No Starch Press styles. If you want to see only the No Starch Press styles, choose **Custom Styles**.



Here are some tips:

- Consider docking the Styles and Formatting window to one side of your OOo workspace. Just drag it off to the very edge and it should dock there.
- Once you've applied some styles (headings and such), you can choose Applied Styles from the drop-down menu at the bottom of the Styles and Formatting window to show only applied styles and reduce the clutter.
- Click the "a" icon to show character styles (EmphasisBold and such).

Dos and Don'ts from Our Editors

Here's a list of some things for you to think about as you write. These are general guidelines and your editor may suggest others as you write. We will read and edit everything that you send in and our comments can be quite extensive.

- HeadAs are your main section headings. Use them to break up the few larger sections in a chapter. HeadBs break up the HeadA sections, and if you have one HeadB in a section, you should probably have more than one HeadB in that section.
- Don't stack headings. In other words, don't stack a HeadA over a HeadB without any text between them. Every heading (including the chapter title) should have text following it, even if it's only a sentence or two, or things start to look very choppy.

- Don't stack notes, figures, tables, code listings, and so on. Your readers don't want your laundry list; they want you to explain things to them.
- Always discuss and explain your figures, tables, code listings, photos, diagrams, and so on. Don't make your readers work to figure out what you're trying to say. They're counting on you to explain it to them. When you insert an object into your chapter, explain why it's there. Talk your reader through it.
- Always call out (that is, reference) your figures, tables, and captioned code listings with in-text references such as "shown in Figure 3-2" so that your reader knows where to look and what relates to what. And make sure that your figures follow their in-text references.
- Use brief captions where possible and keep the detailed explanations in the main text, unless your style is to use detailed captions for all figures, consistently.
- Don't overdo it with notes. You might shoot to use a note every couple of pages or every three pages or so. Notes should call out something unusually important that a reader might want to reference later on.
- Use boxes for asides that are relevant to the discussion but not central to the discussion.
- Be "I" and let the reader be "you." In other words, inject yourself into the book. It's much more fun to read the writing of an individual rather than the somewhat amorphous "we."
- Read the first sentence or two of every paragraph to make sure that your chapter is coherent and that it flows. If things are holding together, you should be able to read the first sentences of each paragraph and get the gist of the chapter.
- Be consistent. Don't throw your reader off unnecessarily. If you always have a certain section in each chapter, don't leave that section out for no apparent reason in another chapter.
- Say what you mean and don't complicate discussions for no good reason. Don't make the readers guess. Tell them what's important and what they should learn.
- If a program offers more than one way to do things, pick one way for your readers. They can always look up the second way.
- When handling code, use Wingdings to highlight the key points in your code and walk your reader through your listings. Don't bother with the extraneous code; even consider snipping it out (and marking it as having been snipped).
- Consider adding comments within your code in addition to using Wingdings if commenting your code seems to work better.
- If your code listings are short, consider just quoting from the code in text.
- Consider using active rather than passive voice throughout your book.

- Avoid abbreviations when possible. Use "and so on" instead of "etc."; "for example" instead of "e.g."; and "that is" instead of "i.e." We want the end product to look like a book and not a technical manual.
- Don't overuse quotation marks. Not everything is a special phrase.
- Always define and discuss new terms at first mention. Do that early and you don't have to do it later because you can assume that your reader is following you. Highlight new terms using the *EmphasisItalic* character style.
- Your first chapter or two should build the foundation of your book. Make sure that your readers are in the same place as you and give them enough of a base so that you can take them places.
- Don't be afraid of using contractions. People speak using contractions, and we want to create the feeling in the readers that you're there and speaking with them.
- If you find yourself using the word "things," ask yourself if you can be more specific.
- Watch for jargon or you're liable to lose your reader.