How To Get Text from an Image Only PDF File Using Linux

How to use free software in Linux to convert image-only PDF files to text.

James Japan Website SSL Issues – Fixed!

Update:

It's now March 12, 2:30 pm in Guam and the SSL issue has been resolved! An hour ago I went back to the control panel and was allowed to enable the free SSL certificate option.

It's March 11, 8:20 AM Guam time, and I am still having problems with SSL since March 8th. The hosting company of this website, Ipage, changed their policy for providing me a free SSL certificate. I had been using a third-party domain name server (Cloudflare) and not the Ipage server, the free SSL certificate was taken away! This has resulted in security warnings when accessing this website. About 30 hours ago I changed the DNS to point back to Ipage, but the change has not been completed yet. I was told it could take up to 72 hours.

Please be assured you are not in any security danger when visiting this site because I am not asking you to submit any sensitive information such as your credit card number. Thank you to those who have recently sent me gifts through PayPal. Your bank information has not been compromised because you

are sending via PayPal and not directly through this website.

James Japan Moved to New Web Hosting Service

Moving jamesjpn.net from Bluehost hosting to Ipage hosting.

WordPress Webmaster Woes

On February 20th for some reason or another after using a utility to clean up this website from junk code, each and every page and post was deleted! Whether it was a bug in the utility, or perhaps a malicious attack by a hacker, I cannot say. I was able to restore most of the pages and posts from a backup file, but I lost several days work, 4 posts including 3 whole books, many editions on other pages and posts, and recent comments. This left me discouraged. But I can only blame myself for not making a more recent backup of the database after so much work.

I may switch to Drupal which I hear has much better security against malicious attacks. At this time, I am experimenting with a Drupal installation on http://gakudo-jpn.net/ One really cool thing that Drupal has is built in ability to publish books into chapters in separate pages! WordPress cannot do that so easily. It needs a third party plugin called Multipage, what this site is using. Third party plugins are subject to bugs that the WordPress developer have no control over.

I believe a bug in a plugin called **WP-Optimize** was the culprit. I uninstalled it.

Another WordPress plugin I uninstalled is WordFence. I find this plugin next to useless. It never really protected this site from malicious hacker code, it only told me about being hacked after the fact! And usually by then the site was infected so bad I could not even view it. Moreover, WordFence filled the database with junk! After removing WordFence, the database sql file was reduced from 60 megabytes to only 12!

I also got rid of WordPress Online Backup. I think it's better to export the database directly from MyPHPAdmin in Cpanel. WordPress Online Backup took a lot of resources and slowed down the site.

WordPress Security: Checking for backdoors

This website and 8 other websites on the server were going off line from time to time. Upon investigation I found all the PHP files of the WordPress installation were deleted! At first I thought a hacker deleted the files. I re-installed the WordPress installation, the theme and all the plugins (a whole day's work for 9 websites!) but a few weeks later the sites went down again. All the PHP files were again deleted.

I wrote the server company (Avahost) and told them of the problem. They informed me that its was *their* anti-virus software that deleted the files

because all PHP files were infected with malicious code!

I didn't believe ALL the files could have been infected and so I bought new hosting with Bluehost and transferred 4 of the websites to it. Lo and behold after a week or so the websites on Bluehost (including this one) started to have trouble. The security plugin Wordfence reported the WordPress installation, theme and plugins were all infected with malicious code! But in this case, there was no antivirus software on the server to delete them. Avahost was telling me the truth!

I did a Google search to learn more about WordPress security. At last I found the culprit! A hacker installed a backdoor in the database. In the list of users I found a user with no name or email but with administrator privileges!! See the image below:

What you see just above the red line should *NOT BE* in ANY WordPress list of Users! A valid user has a name, a username and an email address, but this one does not. If you are a WordPress administrator, my suggestion is for you to check out your list of users and see if anything like the above is in that list. If it is, just delete it. I chose delete the user with all content.

WordPress tricks: Creating a menu on a page using images from a category

My goal was to use WordPress to create a page of images from a category so that I could continue to add more posts to the category and have the page update itself automatically. In order words, I hoped to imitate this HTML page http://www.deeptruths.com/posters/posters.html using a WordPress plugin to avoid all manuel HTML coding hassel.

I did it using two plugins: Widgets on Pages and Ultimate Posts Widget

I had to edit the Ultimate Posts Widget php file to add code just after the

img tag to float the images to the left and add some space around them.

style=”float:left;margin:1em;”

See the result!

Blocking comment spam in WordPress

This blog was using two WordPress plugins to block comment spam, Akismet which is about 97% effective, and SI CAPTCHA Anti-Spam which requires the commentator to type a code he or she reads from an image.

Today I learned of a WordPress plugin that is supposed to be 100% effective called