

Things Might Get Worse!

An open letter to the ordinary citizens and employees at KPMG, Trillian, McKinsey, SARS, SAA, SABC, ESKOM, PRASA, PIC, ANC, and all the others that might be directly or indirectly impacted by recent events.

26 September 2017

The recent shenanigans in our corporate and political spheres are threatening jobs and careers of employees. We might be close to a tipping point, and you might expect the floodgates of corruption, accusations and counter-accusations, and false evidence to burst wide open. There will be collateral damage to ordinary hard-working people like yourselves.

Those responsible for poor decisions and corruption are desperately going to be seeking scapegoats, and pushing the blame onto others. You could get yourself "thrown under the bus" in the fallout.

Please do everything you can, starting right now, to protect yourself as best you can.

What is your best defence?

Evidence. Hard evidence. Hard evidence that is securely timestamped and irrefutable. Just in case you need to expose it in future to defend yourself. Or evidence that you might want to reveal in future as a whistle-blower. Evidence that you can lock away somewhere safely at home. Just in case.

So this letter gives you one practical way to collect and securely timestamp your evidence.

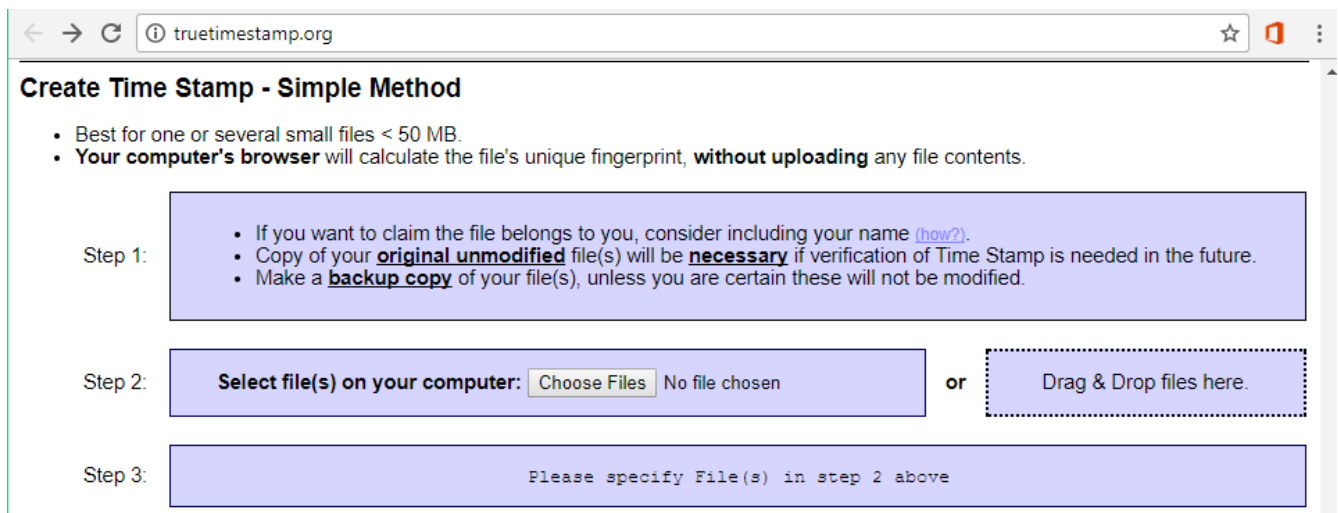
Step 1: Collect some evidence, documents, emails, bank statements, payment requests, write a short report about any threats from your bosses, make a voice recording on your cellphone, take photos or make a video of suspicious meetings, save any emails, if you see an invoice or contract that you have doubts about, try to get a copy, or at least take some photos on your phone. Put the evidence onto a memory stick, or a CD, or onto your phone. (It is probably not a good idea to prepare or leave evidence on your computer at work.)

Put all your evidence into a folder, and zip it up into a single file.

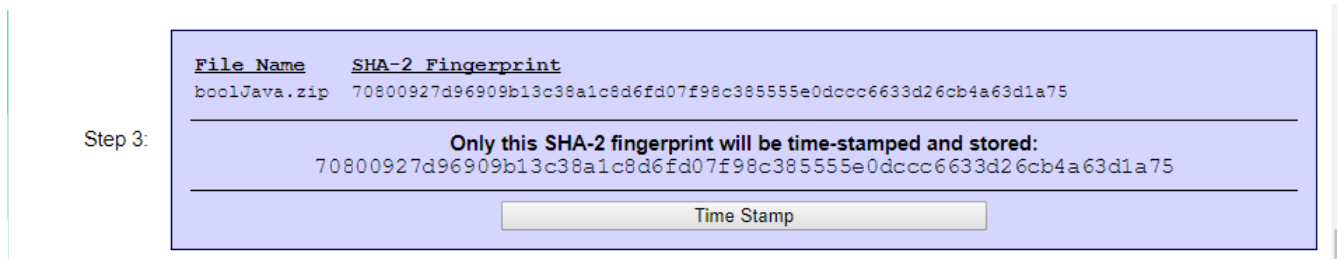
How do I zip it up? Give the evidence folder a sensible name. Then right click on the folder, and **Send To a Compressed (zipped) folder**.

Step 2: Get the zipped file fingerprinted, and get the fingerprint timestamped.

To do this step we are going to use a free public timestamping service. Open <http://truetimestamp.org/> in your browser and scroll down to this section ...



Choose your zip file of evidence, using Step 2 above. This computes a fingerprint for your evidence. It also gives you a button to allow timestamping that fingerprint.



Click the button to request the timestamp, and use the link to download and save the timestamp.

Step 3: Save the evidence (your zip file) and the response from the timestamping service onto a memory stick or a CD and hide it somewhere.

Can you remain anonymous if you release your evidence?

Most software will include information about who created the document, time of creation, name of the computer, etc. So it is very likely that if you reveal your evidence, you'll also inadvertently reveal your identity.

But there are features to let you scrub personal or identifying information from documents. For example, searching for "How do I remove the author from a Word document" will help. But you will need to be very careful. All author information needs to be scrubbed from all evidence before you make the zip file, and then you need to also make sure the zip file doesn't have your author information or your computer name or IP address. Then only should you proceed to the timestamping step.

What should I use this mechanism for?

It has wider applications than just reporting corruption or gathering evidence, or dumping the emails from your email server. If you are the victim of sexual harassment, log the incident by making a short timestamped report. You might want to go public in future if others complain about the same

perpetrator. If you have a great idea like "Please Call Me", write it up and timestamp it before you discuss it with your bosses. If they steal and profit from your idea you will have stronger evidence to challenge them. If your teacher beats you at school, or you're asked to trade sexual favours for better marks in your courses, log the incident. Or if you're a merchant and the SBUX accrediting agent for NSFAS requires a bribe to get your shop accredited for acception SBUX, document and timestamp the incident.

You don't have to disclose anything now, so there is no immedate threat or risk. But if you do choose to strike back in future, you'll be in a stronger position.

And if you're suddenly ordered to work late at the shredding machine destroying contract evidence, bank statements, and invoices, it would be an excellent idea to gather some evidence and document what occurred.

What about files bigger than the 50MB catered for here?

Break the evidence into smaller pieces and timestamp each piece. Or learn how to make your own SHA-2 (also called SHA-256) fingerprint, and use the more advanced section of the same service.

Summary

Things might get worse before they get better. Protect yourself, and contribute to protecting the integrity of our country and its institutions by developing a culture of collecting, timestamping and saving evidence. If the corruption edifice does come tumbling down, you'll be in a stronger position to help.

Regards,

Peter Wentworth (cspwcspw@gmail.com)

The author is a retired academic. He holds a PhD in Computer Science.