How you can preserve digital evidence and why it is important?

Haider M. al-Khateeb and Phil Cobley

Rationale

In a modern ecosystem, your experience in the natural world is highly affected by technology with the cyber space forming an inevitable part of it. This has introduced a whole new range of digital devices and communication channels to your life, some of these are very useful that you probably cannot imagine your daily activities without using them; think about emails, word-editors on your PC or taking a selfie (self-portrait photograph) using the high-resolution camera in your mobile phone. However, this very same technology has unfortunately been used in delicate attacks against you, with Cyberstalking being one of many extreme examples of the risk you may have to face. The good news is: help is at hand!
Further to the psychosocial support you can get while going through this very difficult time, it is vital that you liaise with the police to build a case when the law has been broken if you decide to pursue a prosecution.

Ultimately, it is your choice as a victim of crime whether or not you wish to report the incident, and also whether or not you wish to support any prosecution. Sometimes the Police will decide to pursue a prosecution, even when the victim does not wish to offer their support. However, this will likely only be the case after serious consideration by the Police, and is often based on potential threat, harm or risk concerns that the Police may have either for you or others.

As a victim of Cyberstalking, you could help to construct and maintain digital support for your assertion. It is in your best interests to give law enforcements the chance to acquire evidence that is admissible to a court of law, and in order to ensure that evidence is admissible the Police need to adhere to strict policies and guidelines, following certain procedures and protocols. These can vary depending on the Force who are dealing with the investigation, and they can at times feel inconvenient or unnecessary, but if at any stage you can always speak to the investigator and sometimes even agree compromises to help reduce the impact on you as a victim. This isn't always possible, but investigators will always try their best to accommodate any victims of crime and minimise any negative or intrusive impact that the investigation may cause.

This chapter aims at briefing you with essential key facts and guidelines on how to retain digital evidence(s) of an incident and report that to the police. Please note, this work mainly aims at raising your awareness on the subject matter, it is still recommended that you get advice on your particular case from your local Police Force.

What do you need to know to about digital evidence?

Digital evidence can be defined as any electronic data that is

al-Khateeb, H. M., Cobley, P. (2015) 'How you can Preserve Digital Evidence and why it is Important', A Practical Guide To Coping With Cyberstalking, National Centre for Cyberstalking Research, UK: Andrews UK Limited, pp.50-62.

1. Stored or transmitted (sent or received) in a digital form (binary numeral system) on an electronic device
2. Used to evidence an incident (any event of interest) to an ongoing investigation or to a court of law. It is therefore determined to be relevant to a given case and can be processed as information of value to that case
3. Documented by a Digital Forensics Examiner

For instance, an offensive image sent to your mobile phone via a messaging app could constitute evidence and be forensically retrieved from your phone by the Police. Further examples could include, but are not limited to, logs from your home router, internet browsing history, downloaded files, Windows backups, archives and temporary files of Instant Messaging (IM) services (e.g. Whatsapp, Viber), GPS tracks or Sat Nav data, check-ins (e.g. Foursquare, Facebook), CCTV footage and even logs from a hotel's electronic door locks.

Digital evidence can be large and very informative; imagine seizing a storage volume with the capacity with Terabytes (1 Terabyte equals 1000 Gigabytes) of data. They can be altered, duplicated, latent, damaged and yet difficult to destroy under certain conditions (e.g. deleted files could be recovered from memory). Despite these very distinctive characteristics, digital evidence is accepted in a similar way to contextual evidence. It is therefore equally acknowledged in a wide range of crimes such as fraud, piracy, theft, drug trafficking, rape, homicide, terrorism, harassment and stalking. It is also noted that digital evidence can be used in crimes committed partially online; a stalker could attempt to have both offline and online contact with the victim. In these cases the digital evidence may be required to help complete the full picture of activity and offending.

Key points to remember:

- Digital evidence is trustworthy and accepted in a similar way to traditional evidence so long as it is recovered and handled correctly
- It is wrong to assume that digital evidence is often overlooked
- Digital evidence cannot always be recovered by the Officer who initially responds to or attends a reported incident. To maintain the integrity of that evidence and to ensure it will be admissible at court it should only ever be acquired by a qualified Incident Responder or Examiner, (often referred to as a Digital Forensics Investigator or Examiner) who is trained and accredited to carry out the chosen method of data acquisition.

Where can you locate the digital evidence?

It is usually stored inside the Hard Disk Drives (HDD) or Solid State Drive (SSD) of a computer, Flash Memory of peripheral devices such as mobile phones, USB pen-drives and camera memory-cards; or external storage units including CDs and DVDs. All these are examples of permanent storage technology, which means that you will still find those files you downloaded to your Desktop or USB pen-drive even after restarting your laptop or disconnecting your USB pen-drive from the machine,. This is, of course, until you intentionally or accidentally delete them. However, there is also the data that could be lost the moment you close a software application or shut down Windows (or any other Operating System). Think about all that text you wrote into Notepad without clicking the save option. Another example could be the webpage content that you have viewed and then closed the web browser (i.e. Internet Explorer or Firefox). This data is not necessarily lost, it can be recovered from the computer's volatile memory (e.g. RAM) as part of the forensics investigation process, and then used to complete the tail of information together with the hard disk.

Some digital evidence could be remotely shared from servers (e.g. emails) and cloud services (e.g. Dropbox, SkyDrive and Google Drive), this information can be used too. If you fear a shared file will be deleted by the sender, do not worry, try to download a copy to your device and document what you did and when as if it were a time stamped diary entry, where possible mentioning where you copied it from and to (i.e. "C:\My Documents\Folder\File.txt"). More on documenting incidents in the section titled: "Understand the role of forensics investigators".

In essence, it's important to be aware that digital data of any form could potentially be stored and recovered from any storage media, be it your phone, your laptop, your MP3 player, your cloud storage (i.e. OneDrive or Dropbox), even your Sat Nav.

How can you preserve the digital evidence?

Try to consider and understand the following good practices to preserve digital evidence for your case:

- Since digital evidence can be extracted from both your disk drives and the volatile memory of your device (laptop, mobile etc) as discussed earlier, make sure you hibernate your computer instead of shutdown. This will preserve the content of the volatile memory in the hard disk itself until next system boot.
- The Hibernate button might not be enabled by default in your system, In this case, you are strongly advised to enable this feature. For instance, in Windows 8, this is possible if you use Windows explorer to open the following location:
  Control Panel\Hardware and Sound\Power Options\System Settings
  and then click
  'Change settings that are currently unavailable'
  Now look at 'Shut-down settings' and put a tick on 'Hibernate (Show in Power menu)'
- In the case of mobile phones, you might not have a hibernate option but you can turn off your mobile phone immediately (or as soon as possible) to preserve cell tower location (your location) and stop any possible changes to data on the phone. This is the best option in most cases. Once you turn-off your mobile device, not only do you preserve the state of the data inside, but you also stop any remote communications. Remember, if you have a good reason to think a stalker has obtained remote access to your system, they could destroy evidential data without your knowledge.
- If the evidence is located on your mobile device, but you do not feel happy turning the device off or you have need to keep it turned on and connected to the network then try to take screen shots and/or copy the data to alternative storage to mitigate that risk of remote access. If your device cannot be switched off for whatever reason you need to highlight this to the Police at the earliest opportunity to see if the evidential data extraction can be completed as a priority.
- After you hibernate or turn-off the device, remove battery and disconnect any charging cables. This will prevent any automatic booting.
- Share the details of all the digital devices you own with the police, this will help their team to prepare well for the type of devices from which digital evidence can be extracted.

- If the evidence is held on your Facebook account then you can download a full archive of your account as a snapshot at that particular time and date to help preserve the evidence. This can be very useful given the constantly changing nature of Facebook. You can do this extraction prior to the Police attending. Instructions on how to download an archive copy of your account can be found on Facebook's help pages. If you do this then you should save the files somewhere secure with easy access to then show the Police, preferably not on any hard drives that the Police will likely need to seize/recover, so a USB pen drive or CD/DVD would be best if possible.

What other details should you plan to share?

For the evidence to be professionally acquired by forensics investigators, the device is either seized or a forensic copy is created at the site of the "crime" scene, which could simply be your home. The word 'crime' sounds serious indeed, but this is probably a very fair term to describe an incident that is part of cyberstalking.

Usually, the police require certain powers or a warrant to search and/or seize devices, but in your case as a victim of cyberstalking, you can give your consent and agree to submit your device(s) voluntarily. This can often help to speed up investigations, and as mentioned earlier, sometimes arrangements can be made between you and the Police to try to minimise any inconvenience to you when it comes to the need to extract the data from your devices.

The investigation could involve decoding data and you can help by sharing any relevant passwords or encryption keys. If your Operating System was configured to encrypt user files, then sharing access will be necessary. Further, some of the relevant data (e.g. emails, Google Drive) is stored remotely, access to these can help the case too, and so it is always worth considering a reasonable plan in advance to share all required access to data as the Police may need further consent from you in order to access remotely stored data (i.e. In the "cloud").

Key points to remember:

- Prepare yourself to share some of your passwords and other authentication codes
- You may need to also share device manuals, cables and chargers
- Device interactions with the internet can be analysed to build a picture of the overall activity
- Have ownership of the device(s) you plan to submit to the Police, if the device is not yours, or you're not willing to voluntarily hand over the device then the Police may need to seize the device under their lawful powers
- It is easier to share external memory storage than your devices; it is recommended that you have an external memory configured for your phone, this will enable you to share your memory card with the police instead of giving your phone away every time.
  This is especially handy when you are a victim of stalking and expect to face multiple incidents, it will be impractical to use a new phone for every new incident! Whilst the Police will make every effort to accommodate your needs and try to minimise the time they have your device, this cannot always be guaranteed and so should never be assumed.
- Regularly back-up your phone and retain copies of these back-ups. These will help you restore another handset or your phone if needs be at a later today, and also can help to log a trail of incidence.

What if your evidence files were deleted?

If you have deleted files that you want to produce as evidence, do not worry they might be recoverable. Whilst you can manually restore deleted files in Windows from the Recycle Bin, forensics investigators have tools that could recover deleted (and at times damaged) files beyond this point. For example, with the capabilities of your Operating System, you permanently lose your files at the user-level if you quick-format, or manually delete a file on your USB pen-drive. It is however possible to recover this data with forensics tools under certain conditions. Hence, if you mistakenly delete or format evidence, do not assume you have lost them, but also do not try to recover these yourself. The best action is to isolate the memory card or switch-off the device and ask for a professional opinion. The second you begin to create a new file, save data or download free recovery tools you are risking overwriting this “deleted” data, which may potentially make it unrecoverable.

Key points to remember:

- Deleted data can be recovered under certain conditions.
- The chances of recovering deleted files will reduce if you continue to use that device.

Is it acceptable to copy, move or rename evidence files?

The simply answer to this question is that you should not attempt to do any of these actions. To understand the reason behind this advice you should know that digital evidence is not always in the form of human-readable files such as images and English text files. Instead, there are many (supporting) files created and maintained by software that can be used to provide the forensics examiner with critical information about the cyber environment under investigation. This can include network connections, evidence of spyware installed, log files stored in self-contained databases (e.g. LiteSQL) and Metadata.

Metadata is a concept used to define data stored to describe the content and structure of other files, hence their significance to any digital investigation. Metadata can be used to evidence detail such as the owner of the file, access permissions, time and date of creation, modification time, location on a network and many others. Further to regular files on the computer, webpages and email headers contain metadata too. Therefore, it is very useful to be aware that such artefacts exist and can be analysed but it is rather unlikely that you need to do anything about it except following the guidelines suggested in this chapter to avoid damaging these files.

A practical example of how metadata can be damaged is when you copy a file from your Windows drive to a USB pen-drive formatted with FAT32. Your Windows often panics and shows the following warning message: “Are you sure you want to copy this file without its properties?” This technically means that Fat32 cannot welcome the metadata of the file you are trying to copy, hence, Windows is warning you the picture alone (with no metadata) will be copied to your USB pen-drive.

Key points to remember:

- Do not delete files you do not understand or cannot open
- Do not manually rename or move evidence files from their original location
- Format your memory drives with NTFS whenever possible, they store more metadata about your files

What is supporting-evidence? Can you create one?

The evidence does not have to be limited to its original format, in many cases it is recommended that you take further steps to document a copy of the original using secondary digital devices. The legal system does not confine the investigator to the original, instead, supported copies can be admitted and weighted towards the case.

To demonstrate a practical example from the volatile nature of the cyber space, assume you were sent one or a series of harassing tweets that could be used as an evidence, chances are, these tweets would be removed by the originator at a later time to eliminate the original evidence of that event. This is an example of what can be described as a time-sensitive digital evidence. In such case, document your computer or mobile phone screen with one or more of the following methods

1. Digital camera (photos or video)
2. Print-screen option on your keyboard (prt sc)
3. Print out of that browser page
4. Capture a screenshot of your mobile device

This action is desirable because the digital investigator can then do the necessary to evidence your documentation as an exact copy of the original. In this example, the examiner could:

1. Search Browser history and metadata stored on your computer
2. Utilise online achieve services such as Gnip to recover old tweets. This service has all publically available tweets dating back to the very first tweet from March 21, 2006
3. Extract Metadata from your camera (or printer) to evidence date and time of the picture

How can you preserve a sound (admissible) evidence to a court of law?

Any admitted evidence must be in an identical state to how it was first acquired from the crime scene (or simply your device) wherever it is practicable to do so. Otherwise reasons for any copies need to be fully documented by the Police, and it will be down to the courts as to whether this evidence is admissible or not. After a court of law determine the evidence to be relevant to the case, its authenticity and integrity will be examined. In the case of digital files, and since they can be easily altered or disconnected from supporting metadata, the evidence integrity is mainly challenged. Integrity, authenticity and fully documented continuity is therefore the key driver of what to do (or not to do).

Further, it is a court requirement that the digital evidence is obtained with authorisation. Hence, make sure you have ownership on the devices you submit and support with your consent. Alternatively, the police will have to secure a search warrant in advance for any other devices.

Key points to remember:

- Reserve and reduce changes to the system as discussed in earlier sections e.g. Hibernate. Another example, if you are using a Camera, correct the time and date prior to using it, not afterwards.
- Have ownership on seized devices and give your consent (this will usually be in writing, but the Police will help arrange this with you)
- If any changes have been made to data or files that you're aware of, then keep a handwritten diary of them with times and dates of what has happened and when. This will give the forensic examiner an idea of changes that have been made to the data, which they can often verify and support through their own investigation of the data.

- Develop good understanding of the role of the forensics investigator. This should ideally help you to take the right actions and make informed decisions before they are called.

The following section mainly aims at raising the level of awareness on the general principles maintained by forensics examiners during the digital investigation process.

What do you need to know about the role of the forensics investigator?

In the UK, examiners mainly follow guidelines published by the Association of Chief Police Officers (SCPO), knows as the ACPO principles. They are demonstrated below with comments on how each should affect your behaviour towards the evidence:

> *Principle 1: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.*
>
> *Principle 2: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.*

That competent person is the examiner, you can only help them by reducing the number of times you access the data, chances are, you have probably already opened the file to see what it is. It is understood by Police that this may happen, as you would never be expected to be a digital forensics expert in your own right, but simply try to minimise the chances of changing any data (as per principle 1) by using your devices as little as possible where circumstances allow. In all cases, you are strongly recommended to write down notes to describe your actions with any relevant explanation to justify them. Any small detail could be of significant value to the investigator and they really will value and appreciate your notes. That being said, it is the investigator's job to actually document what the implications of these actions (if any) are on the digital evidence, not you.

> *Principle 3: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.*

This rule apply after the evidence is taken for analysis in a specialised laboratory, you have no influence on any process during this stage. The legal system expects the digital evidence to be examined exclusively by a recognised trained processional, other than in extreme circumstances such as immediate risk to life where an examiner is not available and the examination is time critical

> *Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.*

The sooner they are called the better, this will move the responsibility of preserving digital evidence to a professional. Following this step, try to cooperate and listen to their advice as they will want to not only provide the best victim care that they can, but also secure as much evidence as possible in a manner that retains its integrity, authenticity and continuity so that it is admissible at court

Key points to remember:

- Following the ACPO guidelines increases the admissibility of the digital evidence
- Document your actions to help forensics examiners in their job and support your cause
- Documentation methods include photographs and papers

al-Khateeb, H. M., Cobley, P. (2015) 'How you can Preserve Digital Evidence and why it is Important', A Practical Guide To Coping With Cyberstalking, National Centre for Cyberstalking Research, UK: Andrews UK Limited, pp.50-62.