



Knowledge Powered
by Intelligence™

TII's

Online Investigator's Checklist

Find better online information, in less time, at less cost, with less risk™

The Toddington International Inc. **Online Investigator's Checklist™** is designed to be an active reference guide to assist you with current and future online investigations, and should be used in conjunction with the **Online Research Framework™**.

While this checklist does not provide every possible step you may be required to take during an online investigation, it provides a structured framework and a memory aid to ensure that all important points are included. It is the responsibility of the investigator to ensure that comprehensive notes are maintained detailing investigative steps used, and that evidence is secured appropriately and in the correct manner.

It is important to remember that legislation, case law, and advances in technology may alter the way that certain investigative procedures are carried out, and legal requirements must be adhered to at all times.

It is recommended that you study the checklist prior to beginning your online investigation to ensure that all measures are taken to protect your identity and that of your network prior to commencing your research or investigation via the internet.

- Determine incident type and examine "points to prove".
- Refer to Prosecutor regarding up-to-date case law if required.
- Make an informed choice as to the most effective search tools to use (consider a meta search engine for firstphase search).
- When searching names, consider every possible configuration, including nicknames, usernames, account names, etc.
- Use a collection, collation, and storage tool such as **Zotero** to gather information into folders or collections for further examination and/or dissemination.
- When information (or evidence) is located, capture immediately using screen capture (Ctrl + Print Scr) or your computer's copy and paste feature.
- Consider using screen capturing software such as **Snagit**, **Camtasia**, or **Hunchly** to capture entire online investigations for future evidential purposes.
- Search all information, including email addresses, telephone numbers, images, and media articles.
- Utilize advanced search techniques, including Boolean or enforced term operators, and "forced-phrase" searching.
- Search the Deep Web and locate relevant databases, including electoral registers, telephone directories, business databases, maps, and genealogy sites.



Online Investigator's Checklist

- Search social networking sites and online communities, such as Facebook, Twitter, Instagram, LinkedIn, Tumblr, Classmates, and other friend "reunion" sites, etc.
- Search message forums, groups, and Usenet newsgroups, such as Reddit.
- Search for secondary targets, such as friends, associates, family members, ex-partners, children, etc.
- Search for peripheral information, such as vehicles, previous addresses, images, or information referring to similar or past offences.
- Search media sites, such as Flickr, YouTube, Pinterest, TinEye, Webshots, Photobucket, Vimeo, etc.
- Search blogs and free domain hosting sites such as WordPress and Wix.
- Conduct WHOIS lookups on any IP addresses or domain names located.
- Examine online classified and community sites, such as Kijiji, eBay, Craigslist, and Facebook Marketplace, using names, phone numbers, and email addresses.
- Ascertain physical server locations using traceroute programs.
- Use translation tools to search for information in other languages if necessary.
- Examine the **Internet Archive - Wayback Machine** to locate antecedent information, previous site formats, and early associations.
- Examine robots.txt file exclusion standard to locate "hidden" pages within websites.
- Examine images for background information and explore exif data for date, time, equipment specifications, and GPS coordinates.
- Examine HTML for keywords, images, and "hidden text".
- If a suspect is located, consider whether a forensic examination of their computer system may be required.
- Consider conducting an undercover operation or surveillance (electronic or otherwise) and obtaining a search warrant if required.
- Ensure correct legislation is followed regarding live communication (chat) with suspects or other parties.
- If a proxy server is used, consider legal implications of changing your identity/ location.
- Trace emails to point of origin using most appropriate method.
- Ensure FULL disclosure of all steps taken, proxy servers used, communications with suspects, and authorizations received.

Disclaimer: Please note that our training material and investigator resources do NOT provide guidance on law and legislation in relation to information gathered during the course of an online investigation. Please ensure that you are familiar with appropriate legislation governing collection, analysis, dissemination, and storage of information obtained online relating to individuals, groups, and organizations prior to proceeding with any online investigation.

Toddington International Inc. accepts no responsibility for instructions contained within our training material or investigator resources which are applied inappropriately or contrary to the law, legislation, or guidelines governing your organization, country, or region.



TODDINGTON INTERNATIONAL INC. – The Industry Leaders

Call: +1.604.468.9222 Email: training@toddington.com

www.TODDINGTON.COM