New Zealand
DEFENCE
FORCE
Te Ope Kātua O Aotearoa

Headquarters NZDF
Freyberg Building,
Private Bag 39997,
Wellington 6011, New Zealand

T +64 (0)4 496 0999
F +64 (0)4 496 0869
E hqnzdf@nzdf.mil.nz
www.nzdf.mil.nz

OIA-2019-3562

24 July 2019

Mr Alex Harris
fyi-request-10608-3d199c9d@requests.fyi.co.nz

Dear Mr Harris

I refer to your email of 26 June 2019 requesting, under the Official Information Act 1982 (OIA), information about ZX Security.

Specifically, you asked if the New Zealand Defence Force (NZDF) *has ever employed ZX Security Ltd, to provide training in social media or open source intelligence*. If so, you also asked *for all information relating to, or provided by ZX Security Ltd in relation to the above*.

For the avoidance of doubt, you added that you were *not interested in any work done by* [ZX Security Ltd] *on network security or penetration testing*.

Two units within the NZDF, the Explosive Ordnance Disposal (EOD) Squadron and the Military Police, sent members (three people in total) to a two-day course run by ZX Security in the middle of 2015.

There are three main documents relating to or provided by ZX Security. There were in addition a few limited-circulation internal emails inquiring about interest in attending the Advanced Open Source Intelligence Course and the eventual granting of funding approval for attendance at the Course, and so on.

Two documents were provided by ZX Security prior to the conduct of the Course and the third was a debriefing note written by a member of the Military Police Intelligence Cell, following the conclusion of the Course.

Redactions have been made to the documents under sections 6(a), 6(c), 9(2)(a) and 9(2)(b)(ii) of the OIA. Section 9 redactions were made to protect the privacy of individuals and to protect information that, if released, would be likely unreasonably to prejudice the commercial position of the person who supplied the information. I do not consider the desirability of withholding these persons' names, or course cost information, is outweighed, in the circumstances, by a public interest in making the information available.

Section 6(a) of the OIA states that it is a conclusive reason to withhold official information if its release would prejudice the security of the country. Section 6(c) is that clause of the OIA stating that it is a conclusive reason for withholding information if revealing it would be likely to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences.

I trust that this satisfies your request for official information although you retain a right under section 28(3) of the OIA to ask an Ombudsman to review this response.

Yours sincerely

A.J. WOODS
Air Commodore
Chief of Staff HQNZDF

Enclosures:
1. *Advanced Open Source Intelligence Course*, undated
2. *Advanced Open Source Intelligence Training*, undated
3. *Post Activity Report: NZDF MPIC SNCO Attendance on Advanced Open Source Intelligence Course (AOSINT) 29-30 Jun 15*, dated 1 July 2015

Advanced Open Source Intelligence Course

Costs

S.9(2)(b)(ii)

Training rooms:
I have training rooms available in Wellington, Auckland and Christchurch at a cost of S.9(2)(b)(ii). Although you are welcome to use your own, I would recommend using mine for a number of reasons:

- The computer suite comes fully kitted out with new computers and an Internet connection.

- The internet connection is unfiltered, this is important for elements of the course (using ToR, accessing chat rooms, connecting to mail servers, etc)
- I have VMWare and a custom image pre-installed on the computers which is used as part of the course material
- Tea/Coffee/Snacks are provided throughout the day and Lunch is also provided for all attendees
- It's good to get out of the office and away from distractions / emails / work

Availability
Let me know which month you would like to attend the training and I will let you know what dates I have free.

Additional OSINT Services
In addition to the OSINT Training, I also provide a number of other services you may be interested in

- OSINT Process Development - assisting my clients in the procedural aspects of collecting, storing and processing OSINT in a robust and repeatable manner
- OSINT Investigations - Monitoring of Issue Motivated Groups (IMGs), investigation of companies and individuals or groups of individuals
- Automated Intelligence Gathering - I have developed a platform which can automatically harvest content from facebook/trademe/ebay/twitter/etc based on keyword searches and record/report on the results identified

Let me know if you require any further information on anything I have mentioned.
Cheers, S.9(2)(a)

S.9(2)(a)
Security Consultant - ZX Security Limited
Phone: +64 S.9(2)(a) | Email: S.9(2)(a)@zxsecurity.co.nz Web:
www.zxsecurity.co.nz

ZX SECURITY

s.9(2)(a)
s.9(2) @zxsecurity.co.nz
+64 s.9(2)(a)
www.zxsecurity.co.nz

Advanced Open Source Intelligence Training

COURSE DURATION

- 2 Full Days (09:00—17:00)

LEARNING OBJECTIVES

- Heighten Operational Security (OPSEC) awareness
- Increase the knowledge of attendees regarding Open-Source Intelligence (OSINT) Gathering
- Introduce attendees to the latest tools and techniques used to extract data from OSINT sources to support their day-to-day work activities

PREREQUISITE KNOWLEDGE

A basic knowledge of computers and the Internet is all that is required

WHO SHOULD ATTEND?

- Law Enforcement Personnel
- Corporate Security Professionals
- Fraud Investigators
- Auditors and Analysts
- Recruiters
- Background Check Professionals

REQUIREMENTS

- ZX Security will provide training room facilities, modern computers and Internet connectivity to host the training
- Facilities are available in Auckland, Wellington and Christchurch

ABSTRACT

The ZX Security Advanced Open Source Intelligence (OSINT) Training course is delivered as two-day workshop in which we cover the techniques and tools used to conduct successful investigations on the Internet. By the end of the course, attendees will be able to produce relevant, timely and actionable intelligence.

DAY ONE OUTLINE

The course will be run as a series of modules with each module discussing one or more topics. Each topic will include hands-on exercises involving the course attendees where they will gain real-world experience with the tools and techniques discussed. The outline of the first day is as follows:

Operational Security (OPSEC)- Introduction

- An overview of operational security processes and measures

Internet Fundamentals

- An overview of the building blocks of the Internet including IP Addressing, DNS and SMTP

Operational Security (OPSEC) – Remaining Undetected

- Details of the various methods that can be used to mask your IP address and true identity

Evidence Collection

- An outline of the processes used to collect evidence for court proceedings
- Tools, techniques and considerations for the collection of evidence

Open Source Intelligence Gathering

- Details of the open-source and social media sources that can be used to investigate an individual
- Use search engines effectively to find exactly what you are looking for
- A run through the tools (open-source and commercial) used for information gathering and analysis
- Details on how to extract meta-data from images including GPS details and device information
- How to connect to and monitor chat rooms and forums (both on the Internet and the Deep Web)

Maintaining Multiple Covert Identities

- Techniques used to identify a fake profile
- How to maintain multiple identities across various social networks
- Techniques for creating a backstop (history) for your online personas
- Systems and processes for sending and receiving anonymous messages

Workshop

- During this workshop the attendees will use the skills gained throughout the first days training to create a detailed dossier on a particular individual or group

Advanced Open Source Intelligence Training

DAY TWO OUTLINE

As with the first day, the second will be run as a series of modules with each module discussing one or more topics. There will be a focus on more advanced topics in the second day, with a particular emphasis on mobile social networks. The second half of the day will cover the automated harvesting of content from social networks using techniques that don't require knowledge of computer programming. The outline of the second day is as follows:

Emerging Social Networks

- Sources for identifying new and emerging social networks
- Identification and classification of emerging social networks
- Analysis and overview of new social networks (ask.fm, kik, secret, shots, snapchat, wechat, we heart it, tinder, medium, vine, bubblews, whisper, etc)

Mobile Emulation

- Comparison of Mobile Phone Emulation environments
- Tools for connecting to social networks that are typically only available on mobile phones using your computer
- Techniques to collect information from emulated environments

Automated Harvesting of Content

- Techniques for harvesting information from social networks and other sources with minimal programming knowledge
- Tools and techniques for identifying patterns in data collected from OSINT
- Issues to watch out for when automating information harvesting and solutions to these problems.

Workshop

- During this workshop the attendees will use the skills gained throughout the second days training to create a detailed dossier on a particular individual or group

MILITARY POLICE INTELLIGENCE CELL
NZDF MILITARY POLICE UNIT
MINUTE

3500

01 Jul 15

NZDF MP (Attention: CO)

For Information:
NZDF MP (Attention: XO)
NZDF MP (Attention: OPS WO)

POST ACTIVITY REPORT: NZDF MPIC SNCO ATTENDANCE ON ADVANCED OPEN SOURCE INTELLIGENCE COURSE (AOSINT) 29-30 JUN 15

1. Over the period 29-30 Jun 15, I attended the AOSINT course hosted by EOD SQN and run by s.9(2)(a) of ZX Security.

2. AOSINT Courses costs were s.9(2)(b)(ii) for the training suite used to facilitate the training.

3. The individual course costs and training suite costs were covered by EOD SQN and DIA, with my attendance being free in recognition of my assistance in facilitating the course and some additional training opportunities that fell out of this course for the provider.

4. The course consisted of 2 x EOD s.6(a) pers and 1 X DIA Intelligence Officer.

Background:

5. The Advanced Open Source Intelligence (OSINT) Training course is delivered as a 2 day training package. The training covers techniques and tools used to conduct successful investigations using open source data retrieved from a targets online foot print. On completion of the training participants will be able to produce relevant, timely and actionable intelligence.

Topics covered include:

Day one:

- Internet fundamentals
- Operational Security
- Evidence Collection-Tools, Techniques and considerations for court proceedings
- Open Source Intelligence Gathering-Internet and Deep Web
- Maintaining/Identifying Covert Identities across various Social Networks

Day two: (Enhanced)

- There is a focus on the second day on more advanced topics, with a particular emphasis on mobile social networks.
- Emerging Social Networks-Analysis and overview of new social networks
- Mobile Emulation-Collection of information from emulated environments
- Automated Harvesting of Content-Tools and techniques for identifying patterns in data collected from OSINT

Key takeaway points

6. The training covered a number of skills, applications and programmes that are freely available online that can add real value to the work conducted by NZDF MPIC and ECL in support of investigations where there is intelligence and potentially evidence that can be gained via OSINT methodologies.

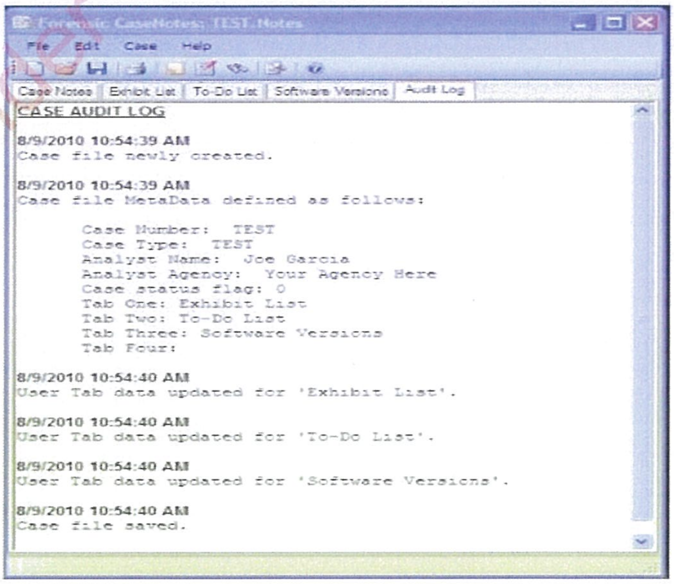
In particular:

- Copies of Association of Chief Police Officers (ACPO) policies on Digital Evidence, and NYC Police OSINT doctrine.

- **QCC Forensic CaseNotes:** http://www.qccis.com/forensic-tools.

  A program that allows an examiner to securely record their digital notes. It runs on the Windows platform.

- It allows for a "write once, read many" data capture
- Date and Time stamps for each entry
- Configuration of case meta-data (case number, examiner name, agency address, etc.)
- An audit log of data entry
- It uses AES 512bit encryption as an option to further secure data



```
CASE AUDIT LOG

8/9/2010 10:54:39 AM
Case file newly created.

8/9/2010 10:54:39 AM
Case file MetaData defined as follows:

       Case Number:  TEST
       Case Type:  TEST
       Analyst Name:  Joe Garcia
       Analyst Agency:  Your Agency Here
       Case status flag: 0
       Tab One: Exhibit List
       Tab Two: To-Do List
       Tab Three: Software Versions
       Tab Four:

8/9/2010 10:54:40 AM
User Tab data updated for 'Exhibit List'.

8/9/2010 10:54:40 AM
User Tab data updated for 'To-Do List'.

8/9/2010 10:54:40 AM
User Tab data updated for 'Software Versions'.

8/9/2010 10:54:40 AM
Case file saved.
```

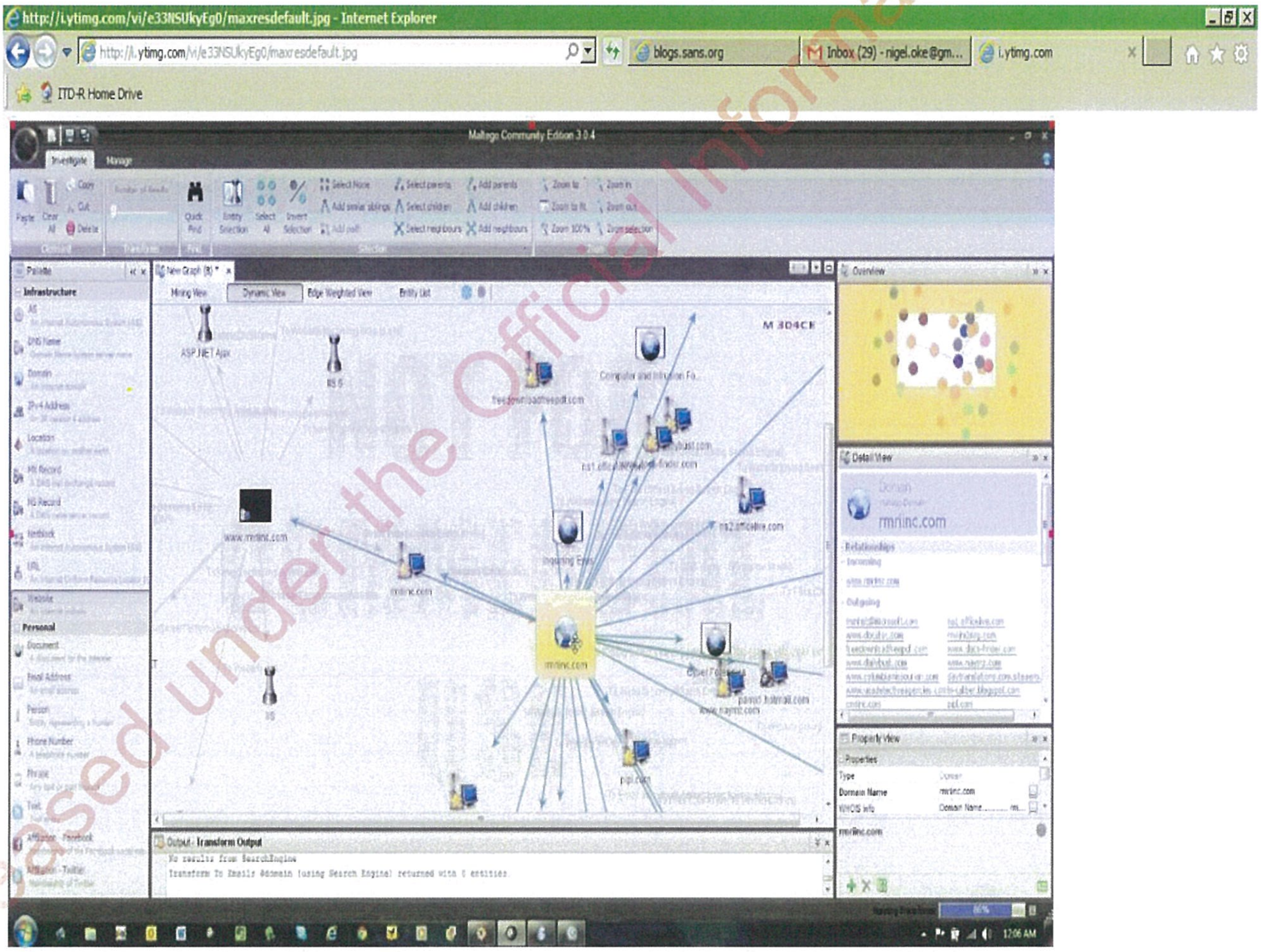
- The use of FACEBOOK Graph Search to accurately define searches within Facebook using multiple terms ie. S.6(c).

- The use of FACEBOOK developer's tools to extract all comments and posts from a particular GROUP (s.6(c)) and convert the online data into Excel spread sheet form for key word searching and analysis.

- **Maltego:** https://www.paterva.com/

  Maltego is free software used for open-source intelligence and forensics, it focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining similar to I2 Charting.

  The basic focus of the application is analyzing real-world relationships between people, groups, websites, domains, networks, internet infrastructure, and affiliations with online services such as Twitter and Facebook.



```
Output - Transform Output
No results from SearchEngine
Transform To Emails @domain [using Search Engine] returned with 0 entities.
```

SCUMBLER: http://techblog.netflix.com/2014/08/announcing-scumblr-and-sketchy-search.html

- This is a freely downloadable application. Many security teams need to stay on the lookout for Internet-based discussions, posts, and other bits that may be of impact to the organizations they are protecting. These teams then take a variety of actions based on the nature of the findings discovered.

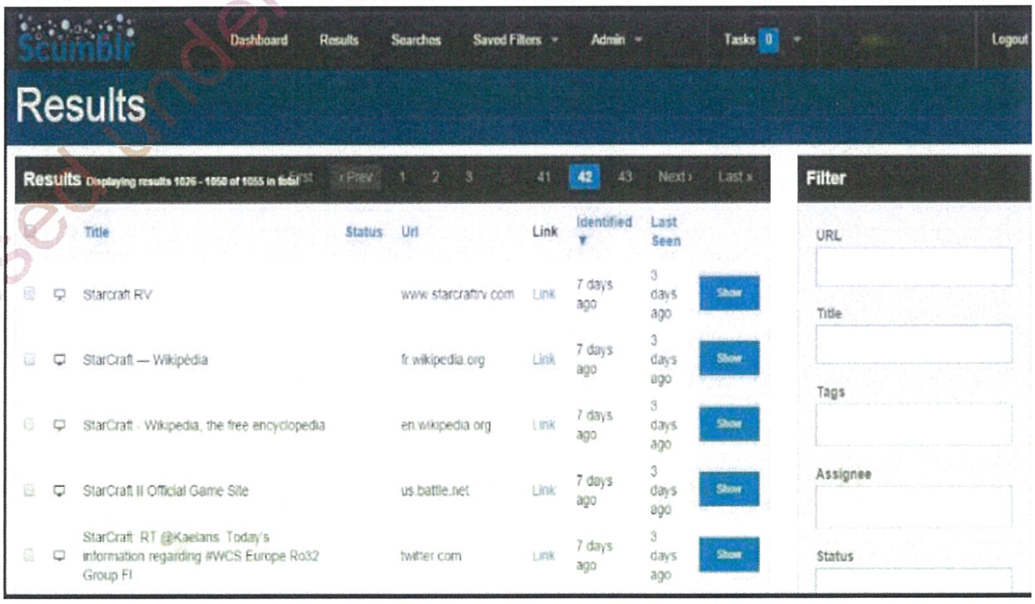
- Scumblr is an application that allows searching the Internet for sites and content of interest. Scumblr includes a set of built-in libraries that allow creating searches for common sites like Google, Facebook, and Twitter. For other sites, it is easy to create plugins to perform targeted searches and return results.

- Once you have Scumblr setup, you can run the searches manually or automatically on a recurring basis. This application is set and forget, it emails you a list of all hits across all identified target sites daily and allows you to capture the exact link/ref forensically and then forward that data to whomever you chose.

- This would allow NZDF MPIC to use the application to target in on specific FB sites of interest and programme in key words to report back on. For example:

S.6(c)

***Note:** This is a significant new issue facing NZDF. Facebook cannot be monitored or enforced in the same way we currently identify potential s.6(c) and as such these FB sales sites are becoming the location of preference for criminals to trade commodities.



Results

Results Displaying results 1026 - 1050 of 1055 in total

Title	Status	Url	Link	Identified ▾	Last Seen
Starcraft RV		www.starcraftrv.com	Link	7 days ago	3 days ago
StarCraft — Wikipédia		fr.wikipedia.org	Link	7 days ago	3 days ago
StarCraft - Wikipedia, the free encyclopedia		en.wikipedia.org	Link	7 days ago	3 days ago
StarCraft II Official Game Site		us.battle.net	Link	7 days ago	3 days ago
StarCraft: RT @Kaelaris: Today's information regarding #WCS Europe Ro32 Group F!		twitter.com	Link	7 days ago	3 days ago

Resources Provided:

7. I was provided with a copy of the PowerPoint presentation used over the two day period complete with all links and training scenarios. This resource has been saved into the NZDF MPIC folder. This will allow me to have a very detailed reference guide and to provide some specific training/revision opportunities to MPIC and ECL.

Recommendations:

8. I would make the following recommendations:

Recommendation One:

NZDF MPIC be given scope to take our current stand alone Internet PC and make it completely free from any NZDF connection via the use of a prepaid top up data account system (Vodafone or Similar).

This would allow NZDF MPIC the ability to use that resource completely independently of any connection (both physically and organisationally) to NZDF IOT allowing the freedom to use and download some of the tools identified.

Recommendation Two:

NZDF MPIC conduct scoping work and produce a discussion paper around the implementation and customisation of SCUMBLR to create a product designed to meet the needs of NZDF MP in relation to online monitoring of illegal activities, intelligence, and the s.6(c) from multiple online sources.

S9(2)(a) is available for consultation and design of detailed and specific plugins tailored to NZDF/NZDF MPIC targeted searches, as well as providing a real time demonstration of the application to NZDF MP HQ using results from NZDF key word searches in s6(c).

There is potential for this product to be utilised by both NZDF MPIC and DDS (if they do not have something similar).

Summary:

9. This was a great course to have attended and the learning outcomes will add significant value to the overall skill set within NZDF MPIC and ECL. There is a real opportunity to develop a system via SCUMBLR that has the potential to add significant value to NZDF MP outputs.

10. Nothing covered on the course involved any hacking or bypassing of user settings. The tools, tips, and process are simply not known to all and utilise data and information that is freely viewable and obtainable from the internet and as such is not reliant upon authority to seize/use from Commanding Officers for intelligence or evidential purposes.

(Signed on Original)

S.9(2)(a)
S.9(2)(a)
NZDF MPIC

DTelN Phone: S.9(2)(a)