

WELLINGTON REGISTRY

Under The Judicature Amendment Act 1972, Part 30 of
the High Court Rules, the Bill of Rights Act 1990,
and the Search and Surveillance Act 2012

In the matter of An application for judicial review

And in the matter of A search warrant issued by Judge IM Malosi of the
Manukau District Court on 30 September 2014

Between **N A HAGER**
Applicant

And **HER MAJESTY’S ATTORNEY-GENERAL**
First Respondent

And **THE NEW ZEALAND POLICE**
Second Respondent

And **THE MANUKAU DISTRICT COURT**
Third Respondent

Key Evidence Bundle

Volume 2: Respondents’ affidavits

Solicitor	Counsel	
Thomas Bennion	Julian Miles QC	Felix Geiringer
Bennion Law	Richmond Chambers	Terrace Chambers
L1, 181 Cuba Street	L5, General Buildings	No. 1 The Terrace
PO Box 25 433	33 Shortland Street	PO Box 10 201
Wellington 6146	PO Box 1008	Wellington 6143
Tel: +64 4 473 5755	Auckland 1140	Tel: +64 4 909 7297
Fax: +64 4 381 3276	Tel: + 64 9 600 5504	Fax: +64 4 909 7298
tom@bennion.co.nz	miles@richmondchambers.co.nz	felix.geiringer@terracechambers.co.nz

Index to the Key Evidence Bundle

Volume 1: Applicant's affidavits

Tab	Deponent	Date	Page
1	Nicolas Alfred Hager	07.10.14	1
2	Bryce David Edwards	31.03.15	43
3	David James Fisher	27.03.15	62
4	Seymour Myron Hersh	26.03.15	80
5	Gavin Peter Ellis	31.03.15	90
6	Adam Julian Boileau	31.03.15	106
7	Nicolas Alfred Hager (Second)	16.06.15	136
8	David James Fisher (Second)	18.06.15	148
9	Wayne Leslie Stringer	22.06.15	157
10	Adam Julian Boileau (Second)	16.06.15	166

Volume 2: Respondents' affidavits

Tab	Deponent	Date	Page
11	Simon Andrew Beal	04.05.15	191
12	David Christopher Lynch	01.05.15	206
13	Ian Stephen Donovan	30.04.15	220
14	Rex Arthur Cottingham	05.05.15	231

Tab	Deponent	Date	Page
15	Joseph Eng-Hoe Teo	01.05.15	239
16	Brent Peter Whale	01.05.15	251
17	Simon Andrew Beal (Second)	22.05.15	256
18	Joseph Eng-Hoe Teo (Second)	02.06.15	258
19	David Christopher Lynch (Second)	25.06.15	260

Volume 3: Unbundled exhibits

Tab	Exhibit	Reference	Description	Date	Page
11	NAH-1	T1/p14/§51	Guardian and Walkley Magazine articles on <i>Dirty Politics</i> .	24.09.14, and XX.10.14	264
12	DJF-1	T3/p64/§11	NZ Herald articles on warrantless information requests.	01.12.12, 08.12.12, and 25.03.15	268
13	AJB-1	T8/p154/§29	WhaleOil post by Pete claiming to know Source's identity	02.11.14	273
14	AJB-2	T6/p128/§99	One News article in which John Key says he knows source's identity	30.10.14	277
15	NAH-3	T7/p144/§30	Radio NZ article on Police rejection of Greens complaint	01.12.14	278

Tab	Exhibit	Reference	Description	Date	Page
16	NAH-4	T7/p146/§36	NZ Herald article on accusation Cameron Slater attempted to procure a breach of s 249	06.06.15	280
17	DJF-2	T8/p154/§29	Article on burglar not charge after tipping of Police	20.06.13	284
18	AJB-3	T10/p183/§82	Tails software “About” page	13.03.15	285
19	A	T16/p252/§9	Brant Whale’s CV	Undated	290

Volume 4: Key Police Disclosure

Tab	Exhibit	Reference	Description	Date	Page
20	LMC-1 to 15	Affidavits of Linda Marie Cheesman	Extracts from the PD bundles	Various	Original numbering

**IN THE HIGH COURT OF NEW ZEALAND
WELLINGTON REGISTRY**

CIV-2014-485-11344

UNDER THE	Judicature Amendment Act 1972, Part 30 of the High Court Rules, The Bill of Rights Act 1990, and the Search and Surveillance Act 2012
IN THE MATTER OF	An application for judicial review
BETWEEN	NICOLAS ALFRED HAGER
	Applicant
AND	ATTORNEY-GENERAL
	First Respondent
AND	THE NEW ZEALAND POLICE
	Second Respondent
AND	THE MANUKAU DISTRICT COURT
	Third Respondent

**AFFIDAVIT OF SIMON ANDREW BEAL ON BEHALF OF THE FIRST
AND SECOND RESPONDENT**

CROWN LAW
TE TARI TURE O TE KARAUNA
PO Box 2858
WELLINGTON 6140
Tel: 04 472 1719
Fax: 04 473 3482

Contact Person:
Brendan Horsley / Kim Laurenson
Email: brendan.horsley@crownlaw.govt.nz / kim.laurenson@crownlaw.govt.nz

I, Simon Andrew Beal, of Auckland, Detective Sergeant, swear:

1. I am a Detective Sergeant in the New Zealand Police based at the Manukau station. I have been a Police officer in New Zealand for seven years and before that I was an officer in the United Kingdom for thirteen years.

Investigation into the hacking of Cameron Slater's computer system

2. On 19 August 2014 Cameron Slater made a complaint to Police alleging that an unknown hacker had accessed his email, Facebook and Twitter accounts and his blog website. He explained to Police that he had received emails about securing his various email, Facebook and Twitter accounts on 2 March 2014. He told Police that material obtained from this access to his accounts was published in the book *Dirty Politics* written by the applicant and was obtained and published without his consent.
3. As a result of Mr Slater's complaint, Police commenced an investigation into the identity of the hacker.
4. On the 28th August 2014, I was assigned as the officer in charge of investigating the complaint Mr Slater had made in regard to accessing his computer systems for dishonest purpose. Detective Inspector David Lynch the District Crime Manager was to oversee the investigation.
5. As part of the investigation, I became aware that the applicant wrote books of a political nature. I was aware of the publication of *Dirty Politics* in August 2014 and that it made allegations in relation to a number of public figures and as a consequence had received significant media attention in the lead up to the general election.
6. As part of the investigation, I read the book *Dirty Politics*. It was clearly stated in the book that the applicant had received material from the hacker. At page 12 of the book, the applicant records that he received 'out of the blue' a package containing a USB stick that transpired to contain electronic communications between Mr Slater



192

and others. Those communications informed *Dirty Politics*. The applicant said in the book that he 'had no part in obtaining the material' and could not say anything else about its origins.

7. I along with other members on the investigation team reviewed the various comments that the applicant made in the media about the hacking after *Dirty Politics* was published. In particular, we were aware of an interview of the applicant by Sean Plunket on Radio Live on 14 August 2014. During that interview, the applicant said that the hacker was someone personally known to him. He also said that he did not want to disclose the identity of the hacker 'because they would get in trouble with the police and I've promised to keep their identity a secret'. A copy of a transcript made of that interview can be found in the affidavit of Linda Marie Cheeseman ("LMC") at volume one, page 71.
8. The applicant was interviewed by Susan Wood on One News on 17 August 2014. During that interview he said "I was advised by my lawyer that I should return all the materials to my source because a court judgment could come out which might mean I might be forced because it is a book to hand over all the material and expose my source. I've since gone back to my source, I've done that in the last couple of days and I've said can I please start to release the information which I'd very much like to do and the source told me no." A copy of a transcript made of that interview can be found in LMC-1 at p 67.
9. A written statement of complaint outlining the circumstances was obtained from Mr Slater when he returned from overseas. A partially redacted copy can be found at LMC-8 at p 1445.
10. This investigation was a technically challenging one because the alleged offence had occurred many months prior to the reporting of the matter to Police and appeared to have been by person or persons compromising the security of Mr Slater's computer systems to gain unlawful access.

11. Advice and direction was sought from the Police National Cyber Crime Centre ("NC3") who are the subject experts in this type of investigation. The lines of enquiry outlined by the NC3 were incorporated to the investigation as it moved forward. The technical enquiries were to be completed by NC3 and other enquiries were to be completed by the investigation team.

Cameron Slater's Personal Computers

12. On 15th September 2014 I organised for Cameron Slater to hand over his Apple i-mac computer hard drive for forensic examination. I took possession of the Apple i-mac computer and arranged for the computer to be examined by Electronic Crime Lab ("ECL") staff. Detective Teo delivered the computer to ECL and the computer was subsequently examined by ECL. By the time of the execution of the search warrant, I had been informed verbally that nothing of use to the investigation could be found. The report of the examination was completed after the search warrant was executed and indicated that nothing of evidential value which would assist in identifying the hacker was obtained from the forensic examination of the Apple i-mac computer.
13. On the 22nd September 2015 I spoke to Cameron Slater on the telephone in regard to other devices that may have been compromised or may hold evidential material. I was informed by Slater that he has a macbook pro 13" which he purchased new in July 2014 and therefore could not have anything of value from the alleged hacking. I was also informed that his mobile phone has been reset and rebuilt since the date of the alleged hack and also would not hold any data of evidential value.

Whaleoil.co.nz Enquiries

14. I tasked Detective Teo with various investigative tasks, one such task was to conduct enquiries with the host of the website Whaleoil.co.nz. Detective Teo advised me that he had conducted enquiries with this website host. The website had formerly been

hosted in the United States by a company called Linode. Detective Teo advised that because of the problems encountered including Mr Slater failing to pay disputed outstanding fees to the company, Linode had deleted all relevant files and logs in regard to the Whaleoil.co.nz site. It was therefore not possible to do the enquiries Police intended as the material no longer existed. Therefore getting detailed lists of users for the site was no longer pertinent as their relevant access and logs were no longer able to be investigated further.

Wikisend

15. On 10th September Detective Teo conducted enquiries with wikisend in an attempt to identify the IP address, computer or person who uploaded content obtained from Cameron Slater's social media accounts.
16. This enquiry did not provide any material data of evidential value to the enquiry.

Google, Yahoo, Twitter

17. [REDACTED]
[REDACTED]
[REDACTED]
18. [REDACTED]
[REDACTED]
- 18.1 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- 18.2 [REDACTED]
[REDACTED]
[REDACTED] [REDACTED] [REDACTED]

19.

20.

Application for a search warrant

21. On 29th September 2014, Detective Inspector Lynch reviewed the case and approved that I apply for a search warrant over the applicant's house at 73 Grafton Road, Wellington to try and obtain material that would identify the hacker.
22. I reviewed the investigation file and formed the view that I had reasonable grounds to suspect an offence under s 249 of the Crimes Act 1961, accessing a computer system for dishonest purpose, had been committed. I considered there were reasonable grounds to believe that evidential material relating to the offence would be found at the applicant's house. I set out the grounds for those beliefs in the application for a warrant dated 30th September 2014.
23. I was alert to the possibility that the applicant might claim journalistic privilege. Although I did not make specific mention of it in the search warrant application, I considered I had done what I needed to do by alerting the Judge to the fact that the information we were seeking related to the source of the material that formed the basis of Mr Hager's book. It seemed to me at the time that Mr Hager's book had had so much media attention that the Judge must have been aware of who he was and what the book was about. The search warrant application also has notices to be supplied to the subject of the search which details the rights to bring claim of

privilege which were supplied to the Judge with the application. A copy of the advice to occupier document which was supplied to the Judge and subsequently supplied to Ms [REDACTED] Mr Price and Mr Geiringer at 73 Grafton Road Wellington can be found at LMC-3 p 362.

24. Prior to the search warrant I made myself aware of relevant policy documents in regard to search and seizure powers and the procedures to follow when searches involve privileged material.
25. I reviewed the policy in regard to search warrants, production orders and examination orders involving media organisations, I viewed the procedural guidelines to ensure that all practicable parts of the procedure were followed. The procedure for this search warrant being slightly different as the applicant was not part of a larger media organisation but an individual author who had been in communication with and personally knew the suspected offender.
26. I paid particular attention to the procedures to follow when searches involve privileged material and noted "You may still secure the thing to be searched but must not search it".
27. I also reviewed the general policy on search warrants including sections on:
 - 27.1 Entry, announcement and identification requirements,
 - 27.2 What can be searched and seized,
 - 27.3 Searching for and seizing computer material.
28. Particularly in regard to the guidance on search for and seizing computer material, I noted that searches of computer systems allowed officers to use any reasonable measures to access a computer system or other data storage device located (in whole or in part) at the place if intangible material that is the subject of the search may be on that computer system, and further that Police may require a person who owns, leases, possesses or controls the

computer device or system or an employee of such a person, to provide access information(e.g. password) or other information (e.g de-encryption information)

29. I also made myself aware of sections 130, 131, 133, 136, 138, 139, 142, 144, 145, 146, 147 and 148 of the Search and Surveillance Act 2012.
30. I was aware that lines of enquiry to identify the hacker had either not provided material of evidential value or could not be completed for an extended period of time.
31. The hacker had been in communication with the applicant over a period of time and the hacker was personally known to the applicant. I was not aware of any other person that was in the same circumstances of both personally knowing the hacker and being in ongoing communication with the hacker.
32. I reviewed media commentary and it was apparent that the applicant placed significant emphasis on knowing the hacker and that was why the applicant was comfortable to use the information. I believed that if there was a built up and ongoing relationship with the hacker there would be evidence of that communication and meetings with the hacker at the applicants address. I also knew that forensic examination of computer equipment was possible to reveal evidence held electronically whether the person who held the material believed that they had removed it or not.
33. I therefore was of the view that the search warrant was necessary to identify the hacker.
34. I made the application for a search warrant at the Manukau District Court on 30 September 2014. Judge Malosi granted the warrant as sought.
35. [REDACTED]
[REDACTED]
[REDACTED]

36.

Execution of the search warrant

37. Prior to the execution of the search warrant I prepared an Operational Order dated 1st October 2014 which set out the rationale for the search of Mr Hager's address and the method of execution that should be followed. This Operational Order explained the grounds that Mr Hager may use to claim privilege over certain items at his address and the processes that should be followed in dealing with any such claim of privilege. This Operational Order was then forwarded to all relevant Police personnel on 1 October 2014. A copy can be found at LMC-8 p 1519.
38. On 1 October 2014, I travelled to Wellington with one other member of the investigation team Detective Teo.
39. On 2 October 2014 in company with Detective Teo, I held a briefing at Police National Headquarters present was Detective Teo and three Wellington based officers, Detective Abbott, Detective Ferguson and Detective Parsons. In this briefing I covered all the points in the Operational order and emphasised the following points: the importance of all officers behaving in a professional manner, that only as a last resort and if it would necessarily frustrate

the purpose of the search warrant entry will be forced, that any damage caused by Police would be rectified and repaired as soon as possible with the Police remaining there until that was completed, that exhibits obtained would either be returning to Auckland with investigation team unless they were too bulky to be safely transported with officers and that the minimum of disruption was to be caused to any other occupants.

40. In this briefing I further explained that the search warrant had been reviewed by the Police Legal Section and that the Crown Solicitor was aware of the intended search, and that I had the contact details of a lawyer at the Crown Solicitor's office should there be legal issues at the address. I do not waive privilege in respect of the advice received.
41. In the briefing I explained that the grounds for believing there was evidential material was because Mr Hager had stated that he had received a flash drive containing material and constantly reasserted that he personally knew the hacker and had met with and communicated with the hacker on a number of occasions. This was different to other journalists such as Matt Nippert who had to communicate via the Onion Router and use specific software tails which are methods of communication which are more anonymous and covert.
42. Once the briefing was completed we met with a member of the Wellington Police Electronic Crime Lab, we then proceeded to the address and executed the search warrant at 73 Grafton Road. We arrived at 7.40am.
43. We had considered the possibility that the applicant might claim journalistic privilege and how we would need to respond to any claim of that kind. I was aware that if he did so his claim to privilege would need to be determined by a High Court Judge and that we would not be able to access the documents in the interim.



44. As we were aware of the potential for a privilege claim, we had prepared for how to deal with any seized material. We had with us sufficient material to secure items over which privilege was claimed so that they could be sealed with tape. This was so that we could establish that Police would not have access to any of the material where privilege was claimed, after the conclusion of the search.
45. When we arrived at the applicant's house, he was not home. His daughter [REDACTED] was present. Ms [REDACTED] was not fully dressed when we arrived. She understandably wanted to get properly dressed and I asked the only woman officer present, Detective Fergusson, to accompany her while that was done. We considered we could be looking for a small item like a flash drive and I was concerned to make sure that nothing was concealed from us.
46. I spoke to the applicant on the telephone on two occasions. On the second occasion because of the type of concerns he had I asked him if he was claiming journalistic privilege and he said he was. I explained to him that in that case any material we took would be sealed so that Police could not look at them until the legal process was complete.
47. Two lawyers were present for some of the execution of the warrant, Steven Price and Felix Geiringer. Mr Price was present from 9.10am until we left the house. Mr Geiringer was present from 10.40am until approximately 1.30pm.
48. I consider that throughout we executed the warrant in a reasonable way and with a minimum of disruption to Ms [REDACTED] and Mr Hager. Mr Hager spoke to me on the telephone twice but was not present at any stage. I was informed that Mr Hager would return to the address to speak to me by his legal representatives, but that never happened. Ms [REDACTED] was co-operative with Police throughout and was pleasant to deal with. She seemed appreciative of Police's efforts to minimise the disruption.



201

49. During the course of the execution of the search warrant, I provided updates on our progress to Detective Inspector Lynch over the telephone.
50. The search teams were tasked specifically by Detective Teo but were requested to look for any physical documentation which contained contact details such as e-mail addresses and phone numbers of persons, details of meetings with persons or communications with persons who may be linked to the hacker(s).
51. The search had already commenced when it was communicated to me and the search team that there was a privilege claim over the material held at Mr Hager's address. Once that claim of privilege was put forward, I made Detective Teo and the other Police members aware of that claim.
52. Mr Price raised two points with me of concern: a) that of journalistic privilege and b) the address was effectively a working news room and that there should be minimal disruption to Mr Hager's ongoing work as a result of this search.
53. I explained to Mr Price that I was aware of these two concerns but that in order to satisfy the concern of a working newsroom there had to be more consideration of what items for which there was a claim of privilege. It was not possible to rule out material as not being of evidential material without properly searching and reviewing the material at the scene.
54. It was not possible to make any assessment of the physical documents as to their potential to be of evidential value without making the initial assessment of whether they were documents detailing either contacts or communications. Once ascertained these documents were to be pointed out to Detective Teo to be documented where appropriate and sealed. The electronic data could not feasibly be sifted in the same way so it was cloned on site where possible to alleviate the concerns about not disrupting Mr

Hager's ongoing work and where not possible was sealed and secured at the conclusion of the search.

55. During the course of the search, Detective Abbott found a piece of paper with login details and passwords for two online email accounts, these accounts were initially believed to be hotmail accounts but were found to be hushmail accounts. I considered the fact that Mr Hager had access to the username and password indicated that he had accessed the accounts and it therefore fell within the scope of the warrant. I cannot think why someone would have both the username and password for an email account if not to access it. For Police to have accessed the account later would have required a remote access warrant which we never sought to obtain.
56. I also became aware that Detective Abbott had found a piece of paper with what were thought to be details for an account with the Onion Router. A photograph was taken by Detective Abbott of those details and was sent to NC3 for technical assistance. I was aware that advice had been sought from NC3 on what could be done to lawfully secure any contents of that online repository/account but I was not aware at the time that a photograph had been taken. I understand that no further investigation has been carried out using that information.
57. A number of photographs were taken on a camera by Ian Donovan, these photographs were stored on a memory card and that memory card was put in with the sealed material. Detective Teo as officer in charge of exhibits also took photos on his cell phone that were reviewed by Mr Price and Ms [REDACTED] Photographs that they requested to be deleted were deleted with the exception of one photograph which when I explained it was a scene photograph they reviewed again and accepted it not to be deleted. They were not shown photographs taken by Mr Donovan from ECL on a device separate from the camera and memory card as I was not aware of



those photographs. I have not taken any investigative steps in relation to the content of them.

58.

[REDACTED]

59.

[REDACTED]

60.

Any physical documents were recorded on a Property Record Sheet and sealed in brown paper envelopes which were sealed with tape and signed to prevent the material from being seen through the container. Some electronic material was cloned at the house. Other electronic material could not be cloned at the house because it was either encrypted or was too large to feasibly be cloned whilst Police were at the address, so it was also sealed again in either paper or plastic envelopes sealed with tape and then the seals were signed and seized.

61.

At my request, Mr Price signed across the seals to ensure that they could not be tampered with.

62.

It was communicated to me that the applicant was claiming journalistic privilege over all his material so everything that was seized was treated as if journalistic privilege might apply, save for Ms [REDACTED] cell phone. Initially there was no claim of privilege over

the macbook laptop of Ms [REDACTED] and as it had been communicated to us that the impact of this computer being seized would be significant for Ms [REDACTED] studies, a review was conducted with Ms [REDACTED] to ascertain if there was anything of evidential value on the computer. When it was subsequently ascertained there was material on the computer then privilege was claimed over her laptop computer.

63. The search warrant concluded at 6.40pm when we left the applicant's house.
64. All of the material that was seized, or clones of material that was cloned but not seized, was delivered to the Electronic Crime Lab in Wellington for safe storage. It was then delivered to the Auckland High Court for secure storage while the privilege claim is dealt with by the Courts.
65. Apart from two items that were cloned with the applicant's consent so that they could be returned to him, as far as I am aware the seized material remains stored at the Auckland High Court as it has been since first delivered there. Attempts have been made to agree on a process by which the other electronic material could also be cloned and the originals returned to the applicant but it has not been possible to agree on a process which satisfies Police and the applicant.

SWORN

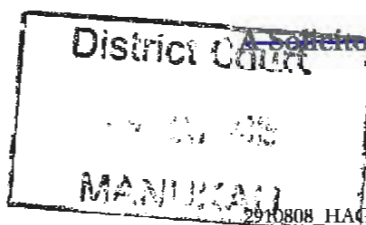
at Auckland this 4th day of
MAY 2015
before me:

P Ngawhika
Deputy Registrar

)
)
)
)



Simon Andrew Beal



~~A Solicitor of the High Court of New Zealand~~

UNDER THE	Judicature Amendment Act 1972, Part 30 of the High Court Rules, The Bill of Rights Act 1990, and the Search and Surveillance Act 2012
IN THE MATTER OF	An application for judicial review
BETWEEN	NICOLAS ALFRED HAGER Applicant
AND	ATTORNEY-GENERAL First Respondent
AND	THE NEW ZEALAND POLICE Second Respondent
AND	THE MANUKAU DISTRICT COURT Third Respondent

**AFFIDAVIT OF DAVID CHRISTOPHER LYNCH ON
BEHALF OF THE FIRST AND SECOND RESPONDENTS
IN OPPOSITION TO APPLICATION FOR JUDICIAL REVIEW**

1 May 2015

CROWN LAW
TE TARI TURE O TE KARAUNA
PO Box 2858
WELLINGTON 6140
Tel: 04 472 1719
Fax: 04 473 3482

Contact Person:
Brendan Horsley / Kim Laurenson
Email: brendan.horsley@crownlaw.govt.nz / kim.laurenson@crownlaw.govt.nz

I, David Christopher Lynch, of Auckland, Detective Inspector, swear:

1. I am a Detective Inspector in the New Zealand Police and the Counties Manukau District Manager Criminal Investigations. I have been a Police officer for twenty-one years.
2. On 25 August 2014, I was made aware that Cameron Slater had contacted Police from overseas alleging that an unknown hacker had accessed his email, Facebook and Twitter accounts and his blog website and that some of that material was published without Mr Slater's consent in the applicant's book *Dirty Politics*. Mr Slater wished to lay a criminal complaint upon his return to New Zealand.
3. Given that Mr Slater resided at that time within the Counties-Manukau Police District, I facilitated the taking of Mr Slater's complaint in the usual manner by having him attend his local Police Station when he returned to New Zealand.
4. Mr Slater attended the Ormiston Road Police Station and completed his statement of complaint on the 29th August 2014.
5. I was aware of who Mr Hager was and knew that he had previously published a book relating to New Zealand politics.

The investigation into Mr Slater's complaint

6. New Zealand Police have a process whereby responsibility for investigating criminal allegations generally lies with the Police District where the offence is said to have occurred.
7. Investigative responsibility for computer generated offending where the location of the offender is unknown is generally assigned to the Police District where the victim was subject to the offending.
8. In this case the location of Mr Slater's computers when they were 'hacked' was within the Counties-Manukau Police District and as such investigative responsibility for this allegation was with the Counties-Manukau Police.

9. It is standard practice for serious crime investigations or investigations of an otherwise sensitive nature to have a higher degree of oversight. Whilst I assigned the file to Detective Sergeant Simon Beal to investigate, I directed that he keep me apprised of the investigation on a regular basis. I was involved in some aspects of decision making on the investigation including the search warrant that is the subject of this judicial review.
10. All complaint files when received are assessed on the basis of information known to see what the appropriate offence category for the allegation is.
11. Mr Slater's complaint was categorised as an investigation into an offence under section 249 of the Crimes Act 1961, accessing a computer system for a dishonest purpose which carries a penalty of seven years imprisonment.
12. As per standard practice, Detective Sergeant Beal compiled an investigation plan with my input which was the basis upon which the investigation was to proceed and would form the basis of his verbal briefings to me on the investigation.
13. Also as per standard practice, although Detective Sergeant Beal was the officer in charge of the investigation, further staff could be utilised as and when necessary to assist in completing various enquiries.
14. The allegation in this case carried a penalty of seven years imprisonment and commensurate with the level of offence, a case of this nature would generally have any obvious and practical lines of enquiry to identify a suspect pursued.
15. Various media commentary and the applicant have suggested that the person known as 'Rawshark' who publically admitted responsibility for the aforementioned crime was acting in the public interest and that the public had the right to know the illegally obtained information.
16. There is no legal 'public interest test' defence to committing a crime. The New Zealand Police do not take into account an 'ends justifies the means' rationale when deciding whether or not to uphold the rule of the law and conduct an investigation. There is however an assessment of whether the public interest test as described in the Solicitor-General prosecution guidelines is met prior to any charging decision.

17. On 15 September 2014, Mr Slater's hard drive was uplifted from him and cloned by staff from the Police Electronic Crime Laboratory so that it could be analysed for anything that might assist Police to identify the hacker. No information that was of assistance was able to be obtained.
18. A twitter account called @whaledump commenced tweeting posts in August 2014. The first tweet was dated 15th August 2014. This account was later identified as being used by the person who had admitted illegally obtaining material from Mr Slater's computer.
19. Police conducted an analysis of *Dirty Politics* and statements made in the media to identify suspects or further lines of inquiry. The applicant said in the media that he knew who the hacker was and had promised to keep his or her identity a secret.
20. I obtained a copy of the book *Dirty Politics* for the purposes of the investigation. It quickly became evident to me that the only part of the book that was relevant to the investigation was the 'Preface' section.
21. There were two points in particular that I noted; (1) The applicant stated that he received 'out of the blue' the illegally obtained documents that he based the book upon on an 8 gigabyte USB digital storage device & (2) that the applicant acknowledged that he had not used 'this type of source before'. I took that to mean that the applicant had not previously received material that he knew had been obtained by a criminal act as opposed to someone who had legitimate possession of the material but chose to 'leak' it.
22. An analysis was done of material available via open source documentation publically available via the internet, including social media and traditional media organisations.
23. The fact that the applicant went further to distance himself from the material in his book by stating 'I had no part in obtaining the material and I cannot say anything else about its origins' is further corroboration in my opinion that the applicant knew the material was obtained by a crime. Statements he made in media interviews also corroborate this fact.

24. Given that the applicant accepts he had not received material obtained from a crime before, his analogies about how Police have dealt with him on prior occasions with material not obtained via a crime are not relevant as they compare two very different situations.
25. Mr Slater's Facebook account was hacked by someone trying to use a particular email address. A production order was obtained over Yahoo for registration details and historical logins for that email address. In that way a related telephone number was obtained. Inquiries were made to establish the person connected to that telephone number. That person was ultimately eliminated from the inquiry.
26. Police conducted a review of open source material looking for people who would have the ability to conduct the kind of hacking that was done here. We also reviewed open source material looking for connections with the names of Rawshark, Whaledump and words associated with this inquiry.
27. Police conducted enquiries with wikiscnd to attempt to identify the person who posted the dumps from the @whaledump twitter account. These enquiries however did not progress the enquiry further.
28. A number of other enquires were completed which were also unable to advance the investigation. Detective Sergeant Simon Beal is in the best position to describe the nature and result of these enquires in more detail.
29. I decided that the applicant should be treated at that stage of the investigation as an uncooperative witness as opposed to a suspect. The reason for my decision in this regard was based largely upon the Court of Appeal decision in *R v Dixon* [CA518/2013]. That decision was subsequently appealed and judgment is pending. It may be that the judgment will have some bearing on whether or not the applicant has himself committed an offence as well as Rawshark.



30. Police made several information requests in relation to the applicant as well as obtaining production orders for his bank accounts. Such enquires are basic steps in many investigations to pursue a variety of legitimate enquiries. In this case no information was obtained that advanced the investigation in terms of identifying the offender.
31. The applicant's bank account details were obtained in order to establish a number of important facts for the investigation. These included to ascertain any travel movements that may have been able to be linked to the offender as well as assessing whether or not he was generating income from the proceeds of the book that could be considered for proceeds of crime action.

Decision to apply for a search warrant

32. By 29 September 2014, some of our lines of inquiry had reached an end. Others were ongoing but were likely some months away from providing us with any information. We therefore considered the next step of the investigation which was applying for a search warrant(s) in respect of the applicant's house or that of other journalists who might have had contact with the hacker.
33. There was a substantial amount of media commentary about '*Dirty Politics*' from a number of journalists. Journalists who had admitted being in contact with 'Rawshark' were the applicant, Patrick Gower, David Fisher and Matt Nippert.
34. The applicant was clearly distinguishable within this group as he was the only person who openly admitted that he knew who 'Rawshark' was as well as being in contact with him. Police knew that copies of the illegally obtained material was almost certainly held by various media organisations and search warrants or production orders could also be considered in respect of these organisations to recover this material as evidential material.
35. I came to the conclusion however that unless there was evidence that suggested any of the aforementioned journalists actually knew the identity of the offender, search warrants for that material would be of limited value to the investigation. Police exercise a degree of caution in executing search warrants on media organisations and at that stage of the investigation I did not feel that this course of action, although legally available, was warranted.

36. Consideration of a search warrant on the applicant however became the next logical step in the investigation in the absence of any information from examining Mr Slater's computer and the Whaledump tweets.
37. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
38. I also understand that even when people are careful not to leave any electronic trail that can be followed by Police, it is easy to slip up. I also considered that in most cases when Police are aware that a person has been in contact with another person recently, it would be reasonable to expect to find some record of this contact or at least some details pertaining to the person contacted. This could include computer contact, phone contact, forensic evidence from items the person had touched or simply a record of a person's name, nickname or phone number being recorded somewhere. In this case 'evidential material' could simply be a link between the applicant and Rawshark.
39. I was also of the view that executing a search warrant at the applicant's address was a course of action that was probable at some stage of the investigation. In fact the only scenario that would negate the need for this course of action would be if 'Rawshark' was apprehended and Police were able to establish a link to the applicant from the offender rather than vice-versa, or if 'Rawshark' pleaded guilty to the offending without the link having been established.
40. In a scenario that involved Police having accumulated sufficient evidence to charge Rawshark and where the charges were contested on an identity basis, the defence would likely attempt to create reasonable doubt by the Police's failure to establish a link between the applicant and the person alleged to be Rawshark. Police would face in my view justified criticism for failing to follow all logical lines of enquiry in not executing a warrant on the applicant in this regard.

41. Likewise in a scenario where Police completed the investigation without executing the warrant and did not have sufficient evidence to charge an offender, Mr Slater would have grounds to complain to the Independent Police Conduct Authority about investigative failings. I would have to accept in that case that Police failed to follow an obvious and logical line of enquiry and could have been subject to criticism.
42. I considered therefore a search warrant should be executed at the applicant's address firstly and warrants in respect of other journalists only considered if that was still required and information suggested that there was a reasonable belief that the hackers identity would be uncovered.
43. I therefore tasked Detective Sergeant Beal with completing a search warrant application that could be reviewed by a legal advisor to ensure that it met the required standard.
44. I also reviewed current Police policy regarding the execution of search warrants regarding Journalistic privilege.
45. In 2014, prior to the warrant on the applicant's address, I approved the execution of one production order and one search warrant where I knew that privilege was likely to be claimed by the subjects of the applications. In both of these cases the type of privilege was legal privilege. Neither was in relation to this investigation.
46. The standard copy of the warrant template that Police provide to both the judicial issuing officer and the subject of the warrant clearly outlines the types of privilege that are able to be claimed and that fact that the subject of the warrant has the right to claim privilege and/or seek legal advice about privilege.
47. The template also gives the judicial issuing officer the opportunity to issue extra conditions around the execution of the warrant if they feel it appropriate.
48. Both of the other applications were granted by District Court Judges and both were executed without any legal challenge as to the lawfulness of obtaining or executing a warrant where privileged material was anticipated to be located. In both cases no information was provided to the District Court Judge at the time the warrant was applied for other than the warrant application and the warrant

itself. In the case of the search warrant the issuing Judge did impose an extra condition upon issuing the warrant and that was to provide him with a report on the execution of the warrant within 40 days of the warrant execution.

49. In both cases Police were able to negotiate a process whereby we obtained information that was relevant to the investigation whilst respecting the privilege claim. In one case there was court facilitation in the process and the other an out of court agreement was reached.
50. My review of Police policy regarding journalistic privilege resulted in me coming to the conclusion that whilst a Policy existed for executing warrants on Media Organisations, no Policy existed for executing a warrant on a self employed journalist at a private address. The Policy on executing warrants on media organisations contained a number of process steps as follows;
 - Obtaining the approval of a member of the Police executive
 - Making the application to a Judge
 - Maintain close liaison with the 'manager' of the media organisation [unless the manager is a suspect or otherwise involved in the subject matter of the warrant]
 - Ensuring that when the warrant is executed that the subject of the warrant was given reasonable opportunity to claim privilege.
 - Ensuring that a process is followed whereby material that is subject to privilege is delivered the court for further determination.
51. Detective Sergeant Beal submitted a search warrant application to me for review. I reviewed the application and was of the view that the application contained more than sufficient information to put before a Judge.
52. I also had the application reviewed by the Police legal section. I do not waive privilege in respect of that advice. Due to my previous experience in executing warrants involving privilege I was very aware of the process involved and this formed part of my verbal briefing with Detective Sergeant Beal on how the warrant would need to be executed should privilege be claimed.

53. Although the Police policy regarding executing warrants on media organisations did not apply in this case, I decided to follow as much of the policy as practical in the circumstances. I obtained the approval of Assistant Commissioner Burgess prior to executing the warrant. The application was made to a Judge not a registrar. The matters pertaining to privilege were addressed.
54. The only step that was not followed was the advance notice to the applicant of the warrant. In my view this was impractical in the circumstances and would prejudice the investigation. In any event the policy expressly had a caveat that this step did not need to be followed if the manager of the organisation was 'otherwise involved in the subject matter of the warrant'. This was clearly the case with the applicant so that part of the Policy did not apply in any event.
55. Detective Sergeant Beal obtained a warrant on 30 September 2014 from the Manukau District Court. The issuing Judge did not impose any extra conditions around the execution of the warrant.
56. Detective Sergeant Beal and other officers then executed it on 2 October 2014. I did not go with the officers to execute the warrant but I received verbal updates from Detective Sergeant Beal by telephone during the day.
57. Since then, the seized material, with the exception of two items released with the applicant's consent, has been held in the High Court at Auckland. We have not been able to continue with our investigation as it relates to that material. No steps have been taken based on information received from the warrant beyond attempting to secure (but not examine) phone data before it is deleted by the relevant telecommunications company. Other aspects of the inquiry continue.

Other matters raised by the applicant

58. The applicant has said in his affidavit that 'in most media or political cases, the Police err on the side of not laying charges and certainly do not turn up unannounced to raid houses or offices'.

59. I note that no charges have been laid in this case. Police are careful in all cases to lay charges only where the evidential sufficiency and public interest tests are met and there is no special rule for 'media or political cases'.
60. The applicant concedes himself that this case is unique in terms of the source of the information received. I am unaware of any other cases where a journalist in New Zealand has knowingly received material obtained from a crime which was used as the basis for writing a book. Indeed the applicant's affidavit suggests that he did more than just receive the material, he actively went out of his way to elicit the material from 'Rawshark' after becoming aware of its existence.
61. In general terms, I have never been involved in a criminal investigation where the Police have given advance notice of the fact we were going to a particular location to execute a search warrant. In my view, to do so would generally be counter-productive and likely to result in evidence being removed or destroyed.
62. The applicant considers that he has been treated differently to other cases. I do not accept that the applicant has been treated any differently from how I would treat any other person given the exact same set of circumstances. Any differences from the normal have been due to the unique set of circumstances in this case.
63. The Commissioner of Police is independent of the government in operational matters. No Member of Parliament or agent of any Member of Parliament has had any influence whatsoever on this investigation. Neither has any representative of any other government agency or foreign government agency.
64. My position provides for a degree of autonomy over the conduct of investigations. I have not received any direction from any member of the Police executive about the conduct of the investigation aside from seeking the approval of Assistant Commissioner Burgess to execute the warrant as per Police policy. I have discussed aspects of the case with Assistant Commissioner Burgess but this was in the context of conversations initiated by me seeking feedback or advice on certain matters. I have also kept him updated on the progress of the investigation.

65. I have reviewed affidavits submitted by the applicant in these proceedings. They generally fall into three categories; (1) media/political commentators (2) The applicant and his daughter (3) A computer expert. Although I did not have the benefit of this material to consider at the time I decided to apply for the search warrant I can say that even if this material was available it would not have affected my decision to apply for a search warrant and execute the warrant in the manner that it was.
66. In my opinion the media/political commentators generally fail to accept that there is a distinction between 'leaked' information and information obtained from a crime. The discussion of the so called 'chilling effect' is based on the premise that people who are in legitimate possession of information may no longer be prepared to pass on or 'leak' that information to Journalists. That argument is not valid in this case as the information did not come from a source of this nature, rather a person who has publically admitted obtaining the information by committing a crime.
67. If the result of Police action in this case was to create a 'chilling effect' or deterrent so that criminals realised that they could not obtain information by committing a crime and give it to journalists without the potential of being identified, this must be in the public interest and not against it.
68. In terms of the applicant's affidavit there is no material that would suggest to me that the search of his computers and other material would be a fruitless exercise. Indeed some of the applicants comments strengthen the view that we could reasonably believe evidential material can be located. For example he confirms that there was material on his computer to start with that he has 'wiped'. He also admits still having in his possession 'very sensitive' documents dating back as far as 2003 with an inference that that source could be identified. He also states that without reviewing all of the documents he is unable to remember all the details of all of his confidential informants which implies that he simply can't remember what information is or is not contained within the material seized.
69. Mr Boileau has made critical commentary in his affidavit that Police overlooked obvious enquires that should have been made prior to considering a warrant on the applicant. A number of these enquiries discuss technical

matters outside my knowledge base and will be addressed by other Police members. I made the decision based on advice that had been received as a result of ECL/NC3 investigations.

70. I have considerable experience dealing with a large number of experts in a variety of fields. I am well aware that there will be a variety of views within each expert community. It is simply impractical for Police to consult every expert who may have a different suggestion or opinion about how a matter under investigation should be advanced.
71. Mr Boileau also suggests that Police should have made enquiries with [REDACTED] about his post on the 2nd November 2014 as he states that he knows who the hacker 'Rawshark' is. He also suggests that Police should have spoken to the Prime Minister in regard to comments he made to the effect that he had been told the identity of the offender.
72. Both of these enquires are irrelevant to the decision to obtain a search warrant for the applicants address. The information from Mr [REDACTED] was not posted on the Whaleoil Blog until a full calendar month after the search warrant was executed and could not be taken into consideration for the search. In any event, Mr [REDACTED] is [or was] an employee of Cameron Slater and says "we've known for months" who Rawshark is. The clear indication is that is a joint knowledge with Mr Slater who has also claimed knowledge of who Rawshark is and Mr Slater has already provided his opinions on this matter to Police.
73. Similarly the Prime Minister John Key made an announcement in late October 2014 a number of weeks after the Search Warrant that he had been informed who hacked Cameron Slater's e-mails. This information could not possibly affect the decision to search the applicants address as it was a number of weeks after the search.
74. I acknowledge that in some cases looking into people that had legitimate access to the computer system in question would be a good line of enquiry. However in this case Mr Boileau's affidavit failed to mention that 'Rawshark' has publically admitted to the crime under investigation and acknowledged that if he is caught he faces seven years jail. People who have had legitimate access to the computer are unlikely to accept that they have committed such a crime and

that statement clearly suggests the person who accessed the documents was an outsider.

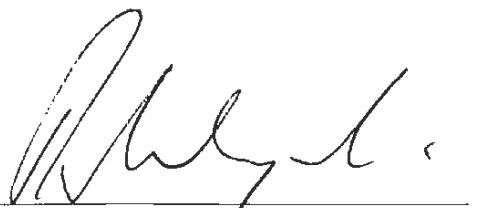
75. Comment has been made about the length of time that Police were at the applicants address and it is accepted that this was about ten hours. The only reason that the search took this long was that Police acted responsibly in respecting the applicant's claim of Privilege. This meant that all items had to be itemised, sealed and signed/countersigned by Police and the applicant's legal representative which was a very time-consuming process. Were it not for this process the search would have easily been completed in far less time.
76. Police accept that the applicant has legitimate concerns about the confidentiality of material that may not relate to this investigation. Police have no interest in any material that is not relevant to this investigation. The applicant is correct however that a full review of all the material seized needs to be conducted to ascertain whether or not it is or is not relevant. This is no different to any other search warrant conducted by Police.
77. It was never anticipated that Police were going to be able to trawl through the applicant's material without any safeguards to address some of the applicants concerns. This is exactly what has occurred in other cases and I had no reason to think that this case would be any different.
78. Police are still willing to have the applicant's material cloned by the Police Electronic Crime Lab and returned to him with the clones returned to storage until the privilege argument is resolved. Such a process would not involve Police actually looking at the material. It could be done with the supervision of an expert instructed by the applicant. I understand he does not agree to that process and accordingly his original material remains seized.

SWORN

at Auckland this 15th day of May 2015

before me:

Phillips


David Christopher Lynch

A Solicitor of the High Court of New Zealand

Christopher Merrick
Solicitor
AUCKLAND

**IN THE HIGH COURT OF NEW ZEALAND
WELLINGTON REGISTRY**

CIV-2014-485-11344

UNDER THE	Judicature Amendment Act 1972, Part 30 of the High Court Rules, The Bill of Rights Act 1990, and the Search and Surveillance Act 2012
IN THE MATTER OF	An application for judicial review
BETWEEN	NICOLAS ALFRED HAGER
	Applicant
AND	ATTORNEY-GENERAL
	First Respondent
AND	THE NEW ZEALAND POLICE
	Second Respondent
AND	THE MANUKAU DISTRICT COURT
	Third Respondent

AFFIDAVIT OF IAN STEPHEN DONOVAN

**CROWN LAW
TE TARI TURE O TE KARAUNA
PO Box 2858
WELLINGTON 6140
Tel: 04 472 1719
Fax: 04 473 3482**

Contact Person:
Brendan Horsley / Kim Laurenson
Email: brendan.horsley@crownlaw.govt.nz / kim.laurenson@crownlaw.govt.nz

I, Ian Stephen Donovan, of Wellington, Digital Forensic Analyst, solemnly and sincerely affirm:

1. Since February 2013, I have worked as a Digital Forensic Analyst within New Zealand Police Electronic Crime Laboratory (ECL) based in Wellington.
2. Between November 2010 and January 2013, I worked at PwC Auckland (formally known as PricewaterhouseCoopers) as a Senior Digital Forensic Analyst.
3. Between March 2008 and July 2010, I worked at IntaForensics Ltd, United Kingdom (UK) as a Digital Forensic Analyst.
4. Between May 2006 and April 2007, I worked at DataClinic (UK) as a Digital Forensic Analyst.
5. I hold a Bachelor of Science Forensic Computing degree with honours (BSc HONS) from Staffordshire University, UK.
6. I am an EnCase Certified Examiner (EnCE), awarded by Guidance Software, Inc.
7. I am a Certified Forensic Computer Examiner (CFCE), awarded by The International Association of Computer Investigative Specialists.
8. I have completed four forensic training courses with Guidance Software in Slough, UK.
9. I have also attended training with Micro Systemation in the use of their mobile forensic system .XRY.
10. I have attended and assisted in about fifteen search warrants.

Prior to search warrant on 2 October 2014

11. On 29 September 2014 I was asked to assist with a search warrant being executed at Mr Hager's house in Wellington. I had no prior involvement with the investigation before that.
12. Before the search warrant was executed I was instructed to contact Detective Sergeant (DS) Simon Beal of Counties Manukau.

221

13. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
14. [REDACTED]:
- 14.1 [REDACTED]
- 14.2 [REDACTED]
[REDACTED]
- 14.3 [REDACTED]
[REDACTED]
15. I understood my role during the warrant would be to assist in identifying devices that may contain data and potentially copy those devices in a forensic manner.
16. At 19:35, I emailed DS Beal outlining what process I would need to take in order to ensure the best evidence was obtained during the warrant, which outlined how I would handle encrypted devices and cloud-based storage.

Search warrant on 2 October 2014

17. At 07:45, I received instructions from Detective Joe Teo to enter the premises.
18. When I entered the premises, I entered into the kitchen / living room area. Directly in front was a steep staircase leading up to the office area and Ms [REDACTED] bedroom. Two computers were located in the office area, one Apple desktop computer and one black desktop computer. A modem (a device that gives access to the internet) was also noted on the desk amongst paperwork.

General concepts

19. A computer may have a hard drive inside of it and that hard drive is responsible for storing data. If preservation of the hard drives data is of importance, then it may be necessary to create a 'forensic copy' of that hard drive to forensic evidence files.

20. It is generally good practice to check a completed forensic copy so that it contains what you expect, this may include reviewing the forensic copy using forensic software and to verify the forensic copy using a hashing algorithm.
21. If a computer system is on and accessible it is an accepted practice to record what is on the screen by photographing the screens contents. Also, a forensic practitioner may copy the computer's memory.
22. It is also good practice to create backups of the forensic copies.

Ms [REDACTED] laptop

23. At 07:54, I was asked by DS Beal to create a forensic copy of Ms [REDACTED] laptop. I understood DS Beal wanted ECL to copy this laptop as soon as possible to avoid disruption to Ms [REDACTED] study (at this point I believed the intention was Ms [REDACTED] would keep her laptop after the warrant).

23.1 Ms [REDACTED] had an Apple MacBook Pro A1278 laptop computer which contained a 500GB hard drive. I began creating a forensic copy of the 500GB hard drive to an ECL hard drive labelled 53247 using a Tableau TD3 forensic duplicator.


23.2 The 'Tableau TD3 forensic duplicator' is forensic hardware capable of forensically copying storage devices, e.g hard drives. Once the forensic duplicator finishes creating a forensic copy it will then verify the forensic copy stored on the ECL hard drive labelled 53247.

23.3 It is possible to use the 'Tableau TD3 forensic duplicator' to preview the exhibit about to be copied, however this was not utilised.

24. At 08:45, I was instructed to stop forensically copying Ms [REDACTED] laptop – instead Detective Teo and Ms [REDACTED] would conduct a review of the laptop's contents. I was then requested by DS Beal to download two email accounts.

Email accounts

25. DS Beal gave me information relating to two Hushmail email accounts and asked me to download them. I understood the search warrant allowed us to

 2023

search for evidential material relating to email accounts that Mr Hager had access to.

25.1 In order to facilitate a legal acquisition of online data, I used the Internet connection available at the search scene, this I understand is the correct process to follow under the Search and Surveillance Act 2012.

25.2 In order to download the email accounts, I had to use Mr Hager's Internet connection, initially I chose to do so using the cable located in Ms [REDACTED] bedroom (as advised by Ms [REDACTED] to be working), however I had trouble using this cable.

25.3 Room to manoeuvre was difficult during the warrant, especially around Mr Hager's office area. Police staff were searching the office area and paperwork and books covered almost every surface. As such, I set up my equipment in Ms [REDACTED] bedroom and used her desk and cable connected to the modem.

25.4 For a period of time, I could not access the modem located in Mr Hager's office area in order to check the wiring and so whilst access was somewhat impractical, I needed to check the Internet settings on my ECL laptop compared with another source, that being Ms [REDACTED] laptop.

25.4.1 I took a photograph of the Internet connection settings on Ms [REDACTED] laptop and used this photograph to confirm I had the same settings on ECL equipment.

25.4.2 The reason why I took the photograph was for my record keeping, so I could continue diagnosing the connectivity issues. It also enabled me to hand back the laptop to Ms [REDACTED] and Detective Teo so they could continue their searching.

25.4.3 The taking of this picture had nothing to do with creating a forensic copy of Ms [REDACTED] laptop, as detailed above, I was instructed to stop doing this.

25.5 The forensic tool I tried to use would have downloaded the email data into a format that is searchable. It would be best practice to check the downloaded data given the volatility of cloud-based data.

25.5.1 Upon successfully downloading the data it would have been sealed with the other evidential material.

25.5.2 As it happens, one email account was deactivated and the other email account was disabled so I could not access anything. I photographed the two screens showing that information using my mobile phone.

25.6 I did not take any further steps in relation to those email addresses.

Backing up Ms [REDACTED] data

26. At around 11:00, I was advised by DS Beal evidential material had been located on Ms [REDACTED] laptop. In order to minimise impact to Ms [REDACTED] study, it was decided to allow Ms [REDACTED] the opportunity to save documents she needed for her studies under my supervision before the exhibit was seized.

26.1 Ms [REDACTED] located a number of documents she needed for her studies.

26.2 I advised Ms [REDACTED] to think beyond her studies and she backed up her CV as she wanted to apply for jobs.

26.3 Ms [REDACTED] burnt the data she needed onto a disc and I suggested to her that she check this disc before we leave. Ms [REDACTED] checked the disc at a nearby family members house.

26.4 I advised Ms [REDACTED] if she thought of any other documents she needed, to let me know as soon as possible.

26.5 In my experience, it is quite uncommon to allow those being searched to back up data, regardless of circumstances, mainly because interactions with a computer system will undoubtedly make irreversible changes.

Mr Hager's computers

27. When we arrived at Mr Hager's house, one Apple desktop computer and one black desktop computer were located and both appeared to belong to Mr Hager and were powered on.

28. Before seizing exhibits that are powered on, it is generally good practice to check to see what programs are running, especially programs relating to encryption.

28.1

[REDACTED]
[REDACTED]

28.2 Both computer systems were locked and the passwords to these systems were provided to Mr Geiringer, a lawyer acting for Mr Hager. However, Mr Geiringer would not provide these passwords to Police.

28.3 Mr Geiringer would not at first unlock the Apple desktop computer because of an adapter he saw that he thought might be a 'key logger' and was touching the equipment and moving wires.

28.4 The device was in fact a PS/2 to USB adapter which allows for an older keyboard to be connected to a USB port. The adapter was not a key logger and without it the older keyboard that was on Mr Hager's desk would not have connected to his Apple desktop computer.

28.5 Mr Geiringer then unlocked the Apple desktop computer after I plugged in the keyboard from the black desktop computer (no adapter required).

28.6 Forensic practitioners would in most situations make efforts to determine whether any type of encryption is running on the computer system, knowing this information will determine how you proceed.

28.7

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

- 28.8 It is also generally good practice to photograph any open documents or webpages before the computer system is shutdown, else this data can be lost.
- 28.9 Material that was open on the Apple desktop computer was photographed by Detective Teo using a camera with a memory card. The memory card was placed with the other seized material. I have not had any access to the memory card since 2 October.
- 28.10 My intention would have been whilst onsite, to forensically copy any computer system that was on and had encryption running. Forensically copying a computer system whilst it is on would not have required me to review the material on the computer.
- 28.11 As it turned out, the Apple desktop computer was not encrypted and the computer system could be shut down.
- 28.12 Mr Geiringer typed various passwords into the black desktop computer in order for Police to gain access to the computer system, however all attempts failed. As a result, we disconnected the computer from its power source. The computer was sealed with the other material seized and I have not had any access to the black desktop computer since 2 October.

The Onion Router (TOR)

29. At approximately 11:30, Detective Abbott provided me a piece of paper which seemed to have details relating to The Onion Router (TOR). I believed that the details on the piece of paper may provide access to evidential material, however I was not sure how to proceed. Detective Abbott was aware that I needed to seek guidance from the National Cyber Crime Centre (NC3) and confirmed I could obtain assistance. I tried calling Technical Investigator Bevan Lee from NC3, however he did not answer. I photographed the piece of paper and emailed it to Mr Lee and asked him to call me. The piece of paper was very detailed and I thought it would be easier to send a photograph of it rather than trying to read it out to someone over the telephone. Mr Lee was not available and eventually Detective Clifford Clark from NC3 advised no

further action was required. I have not done anything with that information since.

Photographs taken on mobile phone

30. During the course of the search warrant I took four photographs on my mobile phone. These were not included with the material that was sealed and sent off to the High Court because I did not appreciate that they could be deemed as privileged, they were however sent via email to DS Beal one week after the warrant with my notes. The photographs were backed up to the ECL network and deleted from my mobile phone the same day. The photographs were as follows:

30.1 One photograph showed the Internet connection settings for Ms [REDACTED] laptop which was taken to assist with diagnosing the Internet connectivity issues I was experiencing.

30.2 Two photographs showed the status of the online email accounts, one being disabled and the other inactive. Assuming I could have accessed the email data, I would not have photographed the screen, instead, I would have downloaded the data which would have been sealed with the other evidential material.

30.3 One photograph detailed TOR instructions.

31. I have not taken any investigative steps in reliance to the photographs taken.

Hard drive containing forensic copies and a memory card containing photographs

32. During the course of the search warrant, I forensically copied a number of devices to an ECL hard drive labelled as 53247. I did not review the forensic copies, nor did I create a backup of the forensic copies made.

33. My understanding was devices to be forensically copied on-site were devices DS Beal thought Mr Hager may need to continue his work and thus were not seized. The following devices were given to me by Detective Teo to forensically copy:

- 33.1 A Toshiba USB storage device (ECL Item # AF140793_2)
- 33.2 An Emtec USB storage device (ECL Item # AF140793_3)
- 33.3 An ADATA USB storage device (ECL Item # AF140793_4)
- 33.4 A DSE USB storage device (ECL Item # AF140793_5)
- 33.5 A Toshiba USB storage device (ECL Item # AF140793_6)
- 33.6 A DSE USB storage device (ECL Item # AF140793_7)
- 33.7 An ADATA USB storage device (ECL Item # AF140793_8)
- 33.8 A non-branded USB storage device (ECL Item # AF140793_9)
- 33.9 An Imation USB storage device (ECL Item # AF140793_10)
- 33.10 An SD card found inside the Panasonic camera (ECL Item # AF140793_11.1)
- 33.11 An Olympus Dictaphone (ECL Item # AF140793_12)
- 33.12 A Kingston USB storage device (ECL Item # AF140793_13)
- 33.13 A Nuix USB storage device (ECL Item # AF140793_14)
- 33.14 A SanDisk USB storage device (ECL Item # AF140793_15) – this device was not forensically copied as it was found to be password protected and was seized along with the other items.
- 33.15 A HP USB storage device (ECL Item # AF140793_17)
- 33.16 An uncased USB storage device (ECL Item # AF140793_18)
- 34. Privilege was not claimed over Ms [REDACTED] mobile phone (ECL Item # AF140793_16) so this was sent to the ECL for immediate processing. Ms [REDACTED] wanted her mobile phone back as soon as possible.
- 35. Detective Abbott hand delivered Ms [REDACTED] phone to my colleague Mr Mark McKnight, a Technical Support Officer of ECL, who extracted data from the

mobile phone using the Universal Forensic Extraction Device (UFED) by Cellebrite.

36. Detective Abbott returned Ms [REDACTED] mobile phone the same day.

Completion

37. While still at Mr Hager's house, I provided DS Beal a hard drive labelled 53247 which contained all forensic copies I had created during the warrant. I also provided the memory card from the digital camera that was used to take photographs.
38. At around 16:30, I left the premises and returned to the ECL.
39. After the search warrant I typed up my notes and sent them through to DS Beal. A redacted version is at LMC-1 at page 129. Other than providing material for discovery, I have not had any involvement with this case since then.

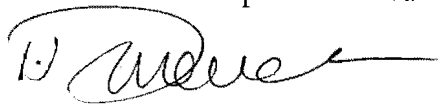
AFFIRMED

at Wellington this 30th day of April
2015
before me:

Ian Stephen Donovan



Joyce Velasco



A Solicitor of the High Court of New Zealand

Deputy Registrar
of the High Court
of Wellington

**IN THE HIGH COURT OF NEW ZEALAND
WELLINGTON REGISTRY**

CIV-2014-485-11344

UNDER THE	Judicature Amendment Act 1972, Part 30 of the High Court Rules, The Bill of Rights Act 1990, and the Search and Surveillance Act 2012
IN THE MATTER OF	An application for judicial review
BETWEEN	NICOLAS ALFRED HAGER
	Applicant
AND	ATTORNEY-GENERAL
	First Respondent
AND	THE NEW ZEALAND POLICE
	Second Respondent
AND	THE MANUKAU DISTRICT COURT
	Third Respondent

**AFFIDAVIT OF REX ARTHUR COTTINGHAM ON BEHALF OF FIRST
AND SECOND RESPONDENTS**

CROWN LAW
TE TARI TURE O TE KARAUNA
PO Box 2858
WELLINGTON 6140
Tel: 04 472 1719
Fax: 04 473 3482

Contact Person:
Brendan Horsley / Kim Laurenson
Email: brendan.horsley@crownlaw.govt.nz / kim.laurenson@crownlaw.govt.nz

I, Rex Arthur Cottingham, of Wellington, swear:

Background

1. I am a Technical Investigator at the Police National Cyber Crime Centre. I have been in this position for 5 years.
2. Before working for the New Zealand Police I spent four years working for Telecom New Zealand where I held two positions of a Security Specialist for Xtra Security and Abuse, and Internet Product Manager. Both roles involved Internet technology and security. While there I developed sound experience in Internet and computer based diagnosis skills and investigation techniques along with management experience. Previous to this I have worked for more than 10 years in the Information Communications Technology (ICT) industry where I have been exposed to a diverse range of technologies, software applications, and network environments.
3. On 28 August 2014 I received an email from Detective Clifford Clark, then acting officer in charge of the National Cyber Crime Centre, asking me to assist in technical inquiries in respect of a complaint made by Cameron Slater about access to his computer. The investigation was known as Operation Oracle. At the time of this investigation the National Cyber Crime Centre had limited resources consisting of a Detective and two Technical Investigators.
4. I provided several technical inquiries to assist with this investigation before the search warrant was executed on 2 October 2014.
5. In any investigation and in particular investigations that involve evidential data, evidence can be lost through damage to hardware, accidental or intentional loss, deletion or overwriting over time. In the case of evidential data relating to attribution, such as identifying an end user linked to an event through an IP address (see explanation below) timing can be particularly acute.
6. Attribution is of particular note as this most often relies on the tracing of IP addresses. As an example, if a computer log is acquired that shows nefarious behaviour and that action on that log is associated to an IP address used at a particular time and date, Police will then be able to identify who the IP address is registered to usually an Internet Service Provider (ISP), Police are then able

to go to that ISP and request information that may lead to identification of a subscriber to whom the IP address was allocated at the relevant time. Police would then need to identify who had access to the internet from the subscriber detail, which in itself is often difficult due to the use of insecure WiFi and multiple users at the relevant location e.g. a library.

7. Information held by ISPs linking allocation of IP addresses to subscribers is often only recoverable for short amounts of time if recoverable at all. IP addresses relating to ISPs or companies offshore are very difficult to obtain and IP addresses used for criminal purposes often relate to offshore proxies or The Onion Ring exit nodes which are near impossible to trace back to a user.

Investigative steps I took

8. On 3 September 2014 I was asked by Detective Constable Paul Stenzel to do some background work on information that he provided me which were IP addresses that were obtained from Mr Slater when his accounts were being targeted. I identified who the IP Addresses were allocated to by using a free online WHOIS lookup service, <http://who.is>.
9. Throughout, I kept a running jobsheet of the steps I took. A redacted copy is attached and marked as Exhibit A.

10. [REDACTED]
[REDACTED]
[REDACTED]

- 10.1 [REDACTED]
[REDACTED]

- 10.2 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

- 10.3 [REDACTED] ■ [REDACTED] ■
[REDACTED]

10.4 [REDACTED]
[REDACTED]

10.5 [REDACTED]
[REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]

10.6 [REDACTED]
[REDACTED]
[REDACTED]

10.7 [REDACTED]
[REDACTED]
[REDACTED]

10.8 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

10.8.1 [REDACTED]
[REDACTED]

10.8.2 [REDACTED]

10.8.3 [REDACTED]

11. [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]
[REDACTED]

11.1 [REDACTED]
[REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]
[REDACTED]

11.1.1

[REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

11.2

[REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

11.3

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

11.4

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED] [REDACTED]

[REDACTED]

11.5

[REDACTED]

[REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

11.6

11.7

11.8

12. Also on 5 September 2014 Detective Sergeant Beal asked me to provide a list of anyone I thought might have the appropriate skill set and technology to carry out this offending. I did not create this list as my view was that this would generate a very long one but I suggested to the investigation team that could be done if they limited themselves to friends and associates of the victim. He also asked me to look for open source material relating to the names Rawshark, Rawshank, Whaledump which yielded negative results in identifying the individuals using those pseudonyms.

13.

13.1

13.2

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

14. In this particular case, the alleged hacking of the whaleoil.co.nz blog was reported to Police on the 29th August 2014 the date of the alleged offence was unknown.
15. It is unknown what weblogs were ever in existence that showed access to the whaleoil.co.nz site. What if any logging did exist they were not available to me at the time of the investigation and in any case may or may not have contained any evidential content as the compromise technique used in this case may have used a technique that would have bypassed the logging process and/or provided access to the logs to the offender who could have easily deleted traces of their identity.
16. Another aspect that needs to be considered is that the login credentials of one of the lawful users may have been compromised, thus hiding unlawful access. It would be impractical to work through each login with each lawful user over several months to identify one or a few unlawful uses.
17. Due to the time delay, loss of data over time, the difficulties on tracing offenders from IP addresses referred to earlier, in my view, even if the access logs were in existence and available to Police, it is likely that those logs would have provided a slim chance of leading to the identity of the person who compromised the whaleoil.co.nz site.
18. I was not present when the search warrant was executed on 2 October 2014.
19. After the search warrant was executed, I have done some further work on this investigation. It has not rested in anyway on material seized from the search warrant conducted on 2 October 2014.

SWORN

at Wellington this 5th day of May)
2015)
before me:)



Rex Arthur Cottingham



A Solicitor of the High Court of New Zealand

Anna Graham
Deputy Registrar
Wellington District Court

UNDER THE	Judicature Amendment Act 1972, Part 30 of the High Court Rules, The Bill of Rights Act 1990, and the Search and Surveillance Act 2012
IN THE MATTER OF	An application for judicial review
BETWEEN	NICOLAS ALFRED HAGER Applicant
AND	ATTORNEY-GENERAL First Respondent
AND	THE NEW ZEALAND POLICE Second Respondent
AND	THE MANUKAU DISTRICT COURT Third Respondent

**AFFIDAVIT OF JOSEPH ENG-HOE TEO ON BEHALF OF THE FIRST
AND SECOND RESPONDENTS**

CROWN LAW
TE TARI TURE O TE KARAUNA
PO Box 2858
WELLINGTON 6140
Tel: 04 472 1719
Fax: 04 473 3482

Contact Person:
Brendan Horsley / Kim Laurenson
Email: brendan.horsley@crownlaw.govt.nz / kim.laurenson@crownlaw.govt.nz

I, Joseph Eng-Hoe Teo, of Auckland, Detective, swear:

1. I am a Detective based at the Manukau Police station attached to the Criminal Investigation Branch, Major Crime Team. I have been a Police officer for 8 and a half years.
2. From Friday 29 August 2014, I have been part of the team tasked with investigating a complaint by Cameron Slater that his computer was illegally accessed.

Investigation before the search warrant

3. Before the search warrant was executed over Mr Hager's house, I was tasked with a number of investigative steps. These tasks are outlined in the following paragraphs.

Twitter – Review and capture of information

4. I was tasked with the daily review of the Twitter account @whaledump and @whaledump2.

On 4 September 2014, I began capturing the Twitter profile @whaledump2. The previous day the Twitter account @whaledump had been deactivated and was no longer accessible.

Facebook enquiry

5. On 5 September 2014, I sent a New Zealand Police Information Request form to Facebook Inc, USA requesting the profile information for Mr Slater's account cam.j.slater and a list of Internet Protocol addresses used to access this account between the dates of 16 February 2014 to 16 March 2014.

5.1 A copy of the original information request can be found at LMC-4 at page 540.

5.2 On 19 September 2014, I received a response from Facebook verifying the personal details for Cameron Slater being associated to the cam.j.slater account. A copy is at LMC-8 at page 1455.

- 5.3 The received information outlined two Internet protocol addresses of 122.56.234.41 and 219.88.138.95 accessing the cam.j.slater account on 10 specific occasions within the specified time period.
- 5.4 Of note, the Internet address 219.88.138.95 was previously identified being linked to Mr Slater through an inquiry made with Orcon as set out later in this affidavit.

Orcon enquiry

6. On 5 September 2014, I was tasked by Detective Sergeant Beal to conduct enquiries with Orcon.
7. Rex Cottingham of the National Cyber Crime Centre identified the Internet protocol address 219.88.138.95 being assigned to Orcon, a New Zealand based Internet Service Provider.
8. On 8 September 2014, I sent an information request to Orcon New Zealand to obtain the account details relating to this Internet address between 16 February 2014 and 16 March 2014.
- 8.1 A copy of the information request sent to Orcon is located at LMC-4 at p 552.
- 8.2 At 4.22 pm, I received a response from Orcon who identified the Internet address 219.88.138.95 being associated to Mr Slater during the requested time period. The response is at LMC-8 at 1485.
9. On 10 September 2014, I sent an email to Wikisend, an American based organisation which maintains an internet based file sharing website. A copy is at LMC-4 at page 577.
- 9.1 The purpose of the email was to identify the computer or person responsible for uploading content obtained from Mr Slater's social media accounts using their online service.
- 9.2 Detective Senior Sergeant Clifford Clark from the National Cyber Crime Centre assisted with obtaining the required information from Wikisend. This resulted with a series of information logs provided to

Police and analysed by Rex Cottingham of the National Cyber Crime Centre.

Production Order – Google, Yahoo, Twitter

10. [REDACTED]
[REDACTED]
- 10.1 [REDACTED]
[REDACTED]
[REDACTED] [REDACTED] [REDACTED]
[REDACTED]
[REDACTED] [REDACTED]
- 10.2 [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]
[REDACTED]
- 10.3 [REDACTED]
[REDACTED] [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Yahoo Production Order Response

11. [REDACTED] [REDACTED] [REDACTED]
[REDACTED]
[REDACTED]
12. [REDACTED]
[REDACTED]
- 12.1 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] [REDACTED]

12.2 [REDACTED]
[REDACTED]

13. [REDACTED]
[REDACTED]

13.1 [REDACTED]
[REDACTED]
[REDACTED]

Twitter Inc Production Order Response

14. [REDACTED]
[REDACTED]
[REDACTED]

Google Production Order Response

15. On 18 September 2014, Google provided a set of data for Mr Slater's Google accounts which can be found at LMC-4 at page 693. The information provided related only to the New Zealand based activity. Google indicated there was activity outside of the New Zealand jurisdiction but required a US court order to obtain the additional information.

15.1 The information provided from Google was sent to Rex Cottingham who identified the internet addresses coming back to Vocus Pty Ltd (an Australian based communications company with a New Zealand office), Spark New Zealand and Vodafone New Zealand.

15.2 After the execution of the warrant at Mr Hager's house, the Internet address linked to Vocus Pty Ltd was identified an account held by Mr Slater. Enquiries with the Vodafone New Zealand did not provide any further lines of enquiry.

15.3 An enquiry with Spark New Zealand (see LMC-4 at page 497) identified the internet addresses provided by Google being linked to

their mobile phone network. A response to this information request was received after the execution of the search warrant at Mr Hager's address.

Cameron Slater imac computer

16. On 15 September 2014, I delivered an Apple imac computer to the Auckland Electronic crime laboratory for examination as tasked by Detective Sergeant Beal.

Nicky Hager enquiries

17. On 24 September 2014, I sent an information request to Spark New Zealand to confirm if Mr Hager held an existing cellular phone account as part of his landline account. That request is at LMC-4 at page 558.
18. A response for this request was not obtained until after the search warrant. Spark confirmed Mr Hager did not hold an existing cellular phone account.
19. On the same day I sent an information request to Vodafone New Zealand verifying if Mr Hager's email address 'nicky@paradise.net.nz' was valid and to provide any details of a cellular phone account link to this email address. That request is at LMC-4 at page 561.
20. Vodafone replied a Production order was required and no further enquiries were conducted.
21. On 26 September 2014, I sent an information request to Trade Me requesting if the organisation held any cellular phone details for Mr Hager. That request is at LMC-4 at page 564.
22. Trade Me replied that a Production order was required in respect to this matter. This line of enquiry was not progressed any further.

Whale Oil website and Linode enquiry

23. On 30 September 2014, I made phone contact with [REDACTED], Mr Slater's technical support person. My note of that conversation can be found at LMC-7 at page 1376.

- 23.1 During this conversation he told me that during February 2014, around the time Mr Slater's social media accounts were illegally accessed, the Whale oil website was hosted on an overseas webhosting service. The company hosting the Whaleoil website was called Linode.
- 23.2 Mr [REDACTED] explained he had basic technical experience with managing a computer server on a daily basis but was not converse with hacking.
- 23.3 During February 2014, Mr [REDACTED] recalls what he refers to as a 'Distributed denial of service' attack on the Whale oil website.
- 23.4 This attack caused the website to be inaccessible for several days. This also included Mr [REDACTED] and Mr Slater being unable to access the Whaleoil website directly themselves.
- 23.5 They made a number of attempts to work with Linode staff to get the Whale oil website up and running again with no success. Mr [REDACTED] made attempts to work with Linode staff to obtain server logs for the Whale oil website and investigate the source of the attack however this was unsuccessful.
- 23.6 Through an indirect method, Mr [REDACTED] managed to copy the Whaleoil website data from the Linode server. He did not copy any files relating to computers and/or Internet addresses which accessed the Whaleoil website.
- 23.7 I asked Mr [REDACTED] about his interaction with Mr Slater's social media accounts. He said he had had no dealings with setting up any of Mr Slater's social medial accounts. Mr [REDACTED] said he had also had no involvement in setting up any of Mr Slater's personal home computer equipment.
- 23.8 Mr [REDACTED] only assumed Mr Slater had secure access to the Whale oil website.

23.9 At the end of our brief conversation, I informed Mr [REDACTED] I would contact him the following week and make arrangements discuss the above points in more detail.

23.10 Further contact with Mr [REDACTED] was made after the search warrant by Detective Sergeant Beal and Detective Constable Smith.

Linode Enquiry

24. Following on from my conversation with Mr [REDACTED] I conducted a telephone enquiry with the American based web hosting service, Linode. Based on what Mr [REDACTED] told me on 30 September 2014 I enquired with Linode directly to ascertain if the server logs were captured by any other means. That inquiry is recorded at LMC-7 at page 1387.
25. Linode explained the company only provides the physical infrastructure for a person to run a website on the Linode servers.
26. Their webhosting service does not hold any historical information relating to Denial of Service attacks in general. The customer service representative informed their systems are attacked daily and to ensure continuity of service they will disable the targeted website being attacked for a period of time.
27. The maintenance of a website is conducted by the account holder of the website, in this case Mr Slater and/or his representatives.
28. Any data relating to the website being illegally accessed and/or attacked would be contained within the 'Virtual Private Server' environment and is not accessible by Linode staff.
29. In this case, the 'Virtual Private Server' data is only held on the whaleoil.co.nz 'Virtual Private Server'.
30. The Linode representative mentioned it was possible for someone who has access to the whaleoil.co.nz 'Virtual Private Server' to copy the VPS data over the internet to preserve the information.
31. Once the account is closed down, all information within the 'Virtual Private Server' is securely deleted and cannot be recovered.

32. Due to the time delay with reporting this incident and investigating the compromise of the Whale oil website, there were no further avenues of being able to retrieve the whaleoil website logs.

Comments on Mr Boileau's affidavit

33. In regards to Mr Boileau's comments at paragraphs 54-60 about investigations that could have been carried out at the scene of the website attack, the initial scene at the time of the website attack was no longer available to the Police investigation team as outlined in the 'Linode Enquiry' section of this affidavit.
34. In response to Mr Boileau's comments from paragraphs 61-75, the initial scene at the time of the website attack was no longer available to the Police investigation team as outlined in the 'Linode Enquiry' section of this affidavit.
35. In response to paragraphs 76-86, as Mr [REDACTED] mentioned to Police, the 'Virtual Private Server' logs in which Mr Boileau outlines was not copied over by Mr [REDACTED] and is inaccessible by Linode staff themselves. This website data at the time of the attack and the VPS logs were deleted shortly after Mr Slater and Mr [REDACTED] moved the Whale oil website to the new hosting provider. By the time the 'Dirty Politics' book had been released there was no chance of the investigation team obtaining this data other than from either Mr Hager himself who had access to this data or otherwise the person who identifies himself as 'Rawshark'.

Execution of the search warrant

36. I was present at the execution of the search warrant at Mr Hager's house on 2 October 2014. My role was to act as exhibits officer.
37. That role involves photographing the scene of the search warrant prior to any search being conducted, documenting the location and providing a description of any items of relevance in accordance to the authorised search warrant.
38. Once the search of the premises is completed and all the items of relevance is identified, I assigned each item a unique item number following the sequence of NH001.

39. I photographed each item in situation on my Police issued iPhone device. Due to the claim of privilege and the impracticality of securely sealing my device, myself, Detective Sergeant Beal, Steven Price and Ms [REDACTED] reviewed each photograph. Any photograph which was deemed to contain sensitive information was deleted.
40. As a result 69 images remain on my iPhone device.
41. During the search, I completed a draft sketch of the premise and identified three main areas to be searched being 1) Bedroom 1 identified as Mr Hager's bedroom 2) Mezzanine floor area identified as Mr Hager's workspace/office area and 3) Bedroom 3 – Bedroom for Ms [REDACTED].
42. At 8.45 am, I was tasked by Detective Sergeant Beal to sit with Ms [REDACTED] and her Apple iMac computer to conduct a number of keyword searches on her laptop. This was to ascertain if her laptop contained any electronic material which fell within the scope of the search warrant.
43. I initially proceeded to note all the emails which returned a result during this tasking but upon further inspection, it was deemed there was electronic material on her laptop which formed part of the 'Dirty Politics' book.
44. At 12.55 pm with the assistance of Electronic Crime Lab analyst Ian Donovan, I recorded the open applications and webpages on the Apple Mac computer located on the mezzanine floor. At this conclusion of this check the computer was 'shut down' and seized. I noted the different cables plugged into this device in my notebook.
45. At the conclusion of the initial search, I particularised each item relevant to the search warrant and assigned them an item number. My notebook entry can be found at LMC-8 at page 1562 and the property record sheet at LMC-1 from p 40.
46. For each electronic device item recorded on site, they were cloned and left at the address at the conclusion of the search warrant. Each cloned item was marked 'cloned' as noted on the Police 268 exhibit form.

47. The items taken away from the address were placed in individual exhibit bags/envelopes according to their assigned item number. Prior to sealing the items, I sat with Steven Price and checked each item in accordance with my notebook and the Police 268 form to ensure accuracy.
48. Mr Price sighted and photographed each item on his own device prior to sealing. Once each individual item was sealed, Mr Price and Detective Sergeant Beal signed each of the seals on each items.
49. At 5.50 pm, I handed over all the seized items which were cloned to Ms [REDACTED]. She confirmed receipt of these items by signing the Police 268 exhibit form. This form was also sighted by Steven Price.
50. In the course of the execution of the search warrant, Detective Abbott drew to my attention a piece of paper that we considered was of interest to the investigation because of information we had already obtained.
- 50.1 It was seized, given the identifying number NH025 and placed with the other seized material. No further investigative steps have been taken as a result of what was seen by myself and Detective Abbott on that piece of paper.
- 50.2 As a result of this proceeding, on 22 October 2014 I wrote a job sheet explaining what had happened in respect of that piece of paper.
51. At the conclusion of the search warrant, all the seized material was sealed and delivered to the Electronic Crime Lab exhibit room in Wellington.
52. On Monday 6 October 2014, I collected the seized items from the Wellington Electronic Crime Laboratory exhibit room and transported them to the Manukau Police station. The items were not removed from the vehicle and the vehicle was secured in the Manukau CIB garage.
53. On Tuesday 7 October 2014, I delivered the seized items to the Auckland High Court and transferred custody of the items to Corrina MacDonald.
54. After the search warrant, I made inquiries to Vodafone and Spark for cell phone records for a phone found in Mr Hager's bedroom.

54.1

[REDACTED]
[REDACTED] [REDACTED]
[REDACTED]

54.2

[REDACTED]
[REDACTED] [REDACTED] [REDACTED]

54.3

If any material had been obtained, we would have had Vodafone send it directly to the Court to be placed with the other privileged material.

Response to [REDACTED] affidavit

55.

During the course of the search warrant I was tasked to conduct a keyword search of Ms [REDACTED] as outlined in paragraph 39 of my affidavit.

55.1

In response to paragraph 19, Ms [REDACTED] was fully informed by Detective Sergeant Beal the requirement for conducting this keyword search under this search warrant.

55.2

As outlined in paragraph 40 of my affidavit, electronic material was located on her laptop in relation to the publication of the 'Dirty Politics' book.

55.3

During this process Ms [REDACTED] was compliant and did not indicate any objection to this particular process.

56.

During the search warrant, Ms [REDACTED] and Mr Hager's representative Steven Price commented during and at the conclusion of the search warrant our professionalism and acknowledged our efforts to ensure privilege was protected.

SWORN

at Auckland this

1st day of May 2015

before me:

A Solicitor of the High Court of New Zealand

Joseph Eng-Hoe Teo

Joshua Martyn
Deputy Registrar
Manukau District Court

UNDER THE	Judicature Amendment Act 1972, Part 30 of the High Court Rules, The Bill of Rights Act 1990, and the Search and Surveillance Act 2012
IN THE MATTER OF	An application for judicial review
BETWEEN	NICOLAS ALFRED HAGER Applicant
AND	ATTORNEY-GENERAL First Respondent
AND	THE NEW ZEALAND POLICE Second Respondent
AND	THE MANUKAU DISTRICT COURT Third Respondent

AFFIDAVIT OF BRENT PETER WHALE

1 May 2015

CROWN LAW
TE TARI TURE O TE KARAUNA
PO Box 2858
WELLINGTON 6140
Tel: 04 472 1719
Fax: 04 473 3482

Contact Person:
Brendan Horsley / Kim Laurenson
Email: brendan.horsley@crownlaw.govt.nz / kim.laurenson@crownlaw.govt.nz

I, BRENT PETER WHALE, Computer Forensic Examiner of Auckland,
swear:

1. I am the director of Computer Forensic Solutions Limited, a company specialising in computer forensic investigations.
2. Computer Forensic Solutions Limited has provided computer forensic services since 2007.
3. Prior to establishing Computer Forensic Solutions Limited, I was employed by the New Zealand Customs Service for 22 years, including 8 years where I was responsible for the Custom Service's computer forensic facility.
4. I am a Certified Forensic Computer Examiner, awarded by the International Association of Computer Investigative Specialists ("IACIS").
5. I am the Director of Standards for IACIS, having been elected to the Board of Directors in 2011.
6. I am an EnCase Certified Examiner (EnCE) awarded by Guidance Software Inc.
7. I have instructed courses in computer forensics in New Zealand, Australia, USA, France, Malaysia, Germany and Croatia.
8. I have given evidence before Courts in New Zealand in criminal matters, for both the prosecution and defence, and civil matters also.
9. A true copy of my CV is annexed and marked "A".
10. I have read, and agree to abide by, the Code of Conduct for Expert Witnesses set out in the High Court Rules. I consider that the evidence I give in this affidavit is within my area of expertise.

Instructions

11. On the 14th of April 2015, I was engaged by the first and second respondents to review the affidavit of Adam Boileau which he had produced in relation to the Nicolas Hager application for judicial review.
12. I was requested to undertake this review due to being an expert witness for computer forensic matters and having experience in conducting investigations.
13. On the 24th of April 2015 I was provided electronic access to the documents that have been provided to the applicant by the first and second respondents.
14. I have also been provided with a copy of the Adam Boileau affidavit dated March 2015.

Review of the investigation undertaken by Police

15. I have reviewed the investigation undertaken by Police up until the point of the execution of the search warrant.
16. I note that Mr Hager is not presently a suspect in the crime being investigated. The application for a warrant to search the Hager premises was because it was believed that reasonable grounds existed to believe that a search of Mr Hager's premises will find evidence relating to that offence. The examination of Mr Hager's electronic storage devices was to

locate evidence of a crime. It was not suspected that these items had been used to commit the crime itself. Mr Hager had stated publically that his book was based on data provided to him on an 8 gigabyte storage thumb drive containing Slater's illegally accessed private communication.

17. In most cases, the ability to recover electronic evidence from a computer itself lessens over time because normal computer usage overwrites the evidential artefacts on the computer. Generally speaking, it is better to obtain electronic evidence sooner rather than later. I note that in this case it seems about six months had passed since the apparent unlawful access.
18. I do note though that the Police Electronic Crime lab received Mr Slaters Apple iMac computer on 15 September 2014 for forensic examination to identify if any malware or system compromise exists even after the time that had passed.
19. Logically, access Mr Hager had to the files must have been more recent than the hacking itself because he received the material from the hacker. Any evidential artefacts on Mr Hager's electronic devices would in any event be different from what the Police could find from the examination of Mr Slaters computers.
20. The Hager artefacts could include any communication between himself and the hacker, or any files that may contain metadata that leads to the hacker. For example, if the Hacker edits a Word document to modify them by removing a sentence or paragraph, then Microsoft Word would record his details as the last author of the document. There are also other ways in which files that came from the hacker might identify the hacker, even if they were being careful.
21. The Slater artefacts could include IP addresses of traffic that accessed the computer that had been compromised.
22. I have considered the technical issues that the Police had to consider before the search warrant was executed on 2 October 2014.
23. It appears to me that the Police file holder took advice from the appropriate experts. These included the Police Electronic Crime Lab who are the experts in the forensic examination of electronic evidence, and the Police National Cyber Crime Centre.
24. These are exactly the two branches of the Police that have the required expertise in the area being investigated. They would have been the same place that I would go to for advice and assistance if I was the Police file holder.
25. [REDACTED]

a. [REDACTED]

b. [REDACTED]

om

[REDACTED]

c. [REDACTED]

d. [REDACTED]

e. [REDACTED]

f. [REDACTED]

g. [REDACTED]

26. These enquiries showed that the Police were not narrowly focused in their investigation and were considering multiple lines of enquiries that had potentially good outcomes in terms of identifying the hacker.

Other avenues of inquiry that have been suggested

27. Some of the suggestions that Mr Boileau make for other inquiries that could be carried out are in my opinion possible lines of inquiry, but should be seen as additional avenues of investigation as opposed to alternative ones.
28. One line of inquiry raised by Mr Boileau is the examination of the virtual private server data held by Linode in the USA. This information may have identified the IP address the hacker was using when the website was compromised. It is likely though that a proxy would have been used which would have masked the hackers true IP address.
29. A proxy is a method of routing internet communication through a virtual private network where no logs are kept of the internet traffic. Using a proxy prevents law enforcement agencies from obtaining the records required to identify the location of an offender such as in this matter.
30. Mr Boileau says this examination would have been at least as likely to show information that might reveal the hacker as any other source of information. I do not accept this statement. Identifying the "hacker" in this manner would be extremely difficult. The hacker would have the ability to mask their true IP address and hence hide their location. I consider the chances of successfully identifying the hacker through examining the virtual private server as low.
31. Mr Boileau suggests in paragraphs 87 – 94 that investigation of the name registry and hosting services should have been considered by the Police. I see nothing to suggest this should have been a line of inquiry. Although this has been a method of obtaining unauthorised access to websites used by some hackers around the world, there is nothing to suggest that this is the case in this matter. The Police need to focus on leads and known intelligence. There is no basis for the Police to make these enquiries.

32. In paragraph 120 Mr Boileau comments on the leaked material already being available in the public domain and there being nothing in those documents to identify the hacker. As I have set out earlier in this affidavit, if the documents were recovered from a search of the Hager premises and they had been edited in some manner by the hacker, then forensic examination may locate metadata evidence indicating who the editing author was.
33. Mr Boileau has set out his views on the possibility of finding evidence considering that special security type software was being used. Mr Boileau states "there is nothing in the documents that have been provided to me to suggest that the Police had any reasonable grounds to believe they would find such material."
34. Encryption and security software has been likened to a safe. While it may be difficult to access the contents of the safe, it is not a reason for an investigation to not proceed. It only takes one error in the use of this security software and evidence can be left on the computer. Computer forensic investigators often locate evidence on computers that the user attempted to remove. Encryption and security software can make this process more difficult, but this is not a reason for the investigation to not take place.
35. Mr Boileau infers that because both the hacker and Mr Hager apparently used Tails software to communicate, that the chances of Police finding evidence at Mr Hager's house were very low. Merely because a person is careful about covering their tracks to not leave a trace of evidence, does not mean that nothing will be found. There may be early communications between the parties before the Tails software was being used. Another possibility is that text was entered into a window that was not protected by the software. The operating system may copy this text into a temporary file which is later located by a computer forensic investigator. Windows operating systems copy data to RAM, swap files and temporary storage locations all the time. It can be very difficult to completely clean all traces of your computer usage.
36. From my independent review of the electronic disclosure relating to the Police investigation up to the time of the search warrant at the Hager premises, I consider that the Police have sort and received expert advice from their National Cyber Crime Centre and their Electronic Crime Lab. The enquiries that they made were both wide-ranging and appropriate.
37. The examination of electronic devices (computers and data storage devices) used by Mr Hager is another obvious and appropriate avenue of investigation that could identify the hacker.

SWORN at Auckland this
1st day of May 2015
before me:

) 
)
)
) Brent Peter Whale


A Solicitor of the High Court of New Zealand

Nicholas Hamilton Birdsey
Solicitor
Auckland

**IN THE HIGH COURT OF NEW ZEALAND
WELLINGTON REGISTRY**

CIV-2014-485-11344

UNDER THE	Judicature Amendment Act 1972, Part 30 of the High Court Rules, The Bill of Rights Act 1990, and the Search and Surveillance Act 2012
IN THE MATTER OF	An application for judicial review
BETWEEN	NICOLAS ALFRED HAGER Applicant
AND	ATTORNEY-GENERAL First Respondent
AND	THE NEW ZEALAND POLICE Second Respondent
AND	THE MANUKAU DISTRICT COURT Third Respondent

SUPPLEMENTARY AFFIDAVIT OF SIMON ANDREW BEAL

CROWN LAW
TE TARI TURE O TE KARAUNA
PO Box 2858
WELLINGTON 6140
Tel: 04 472 1719
Fax: 04 473 3482

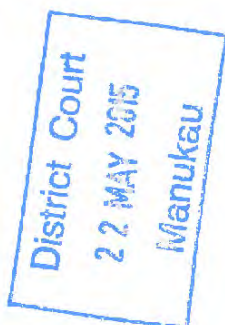
Contact Person:
Brendan Horsley / Kim Laurenson
Email: brendan.horsley@crownlaw.govt.nz / kim.laurenson@crownlaw.govt.nz

I, Simon Andrew Beal, of Auckland, Detective Sergeant, swear:

1. I swore an affidavit in this proceeding on 4 May 2015. I have now realised that the third sentence of paragraph 12 of that affidavit is not correct. Before the search warrant was executed I had been told that it was unlikely that anything could be found on Mr Slater's computer, but I had not been told that it could not be done. I was told that nothing had in fact been obtained from Mr Slater's computer after the search warrant was executed. I have therefore sworn this affidavit to set out the proper position. Paragraph 12 should have read:

On 15th September 2014 I organised for Cameron Slater to hand over his Apple i-mac computer hard drive for forensic examination. I took possession of the Apple i-mac computer and arranged for the computer to be examined by Electronic Crime Lab ("ECL") staff. Detective Teo delivered the computer to ECL and the computer was subsequently examined by ECL. By the time of execution of the search warrant, I had been informed verbally that i-mac computers were highly resistant to malware and compromises and that it was therefore highly unlikely that anything of value to the investigation would be found. I subsequently received another verbal update after the search warrant where I was told that nothing of evidential value to the investigation was found on the computer. The report of the examination was completed after the search warrant was executed and indicated that nothing of evidential value which would assist in identifying the hacker was obtained from the forensic examination of the Apple i-mac computer.

2. I apologise for the error.



SWORN

at Auckland this 22nd day of May 2015

before me:

A Solicitor of the High Court of New Zealand

)
)
)
)

Simon Andrew Beal

**P Ngawhika
Deputy Registrar**

UNDER THE	Judicature Amendment Act 1972, Part 30 of the High Court Rules, The Bill of Rights Act 1990, and the Search and Surveillance Act 2012
IN THE MATTER OF	An application for judicial review
BETWEEN	NICOLAS ALFRED HAGER Applicant
AND	ATTORNEY-GENERAL First Respondent
AND	THE NEW ZEALAND POLICE Second Respondent
AND	THE MANUKAU DISTRICT COURT Third Respondent

**SUPPLEMENTARY AFFIDAVIT OF JOSEPH ENG-HOE TEO ON
BEHALF OF THE FIRST AND SECOND RESPONDENTS**

**CROWN LAW
TE TARI TURE O TE KARAUNA
PO Box 2858
WELLINGTON 6140
Tel: 04 472 1719
Fax: 04 473 3482**

Contact Person:
Brendan Horsley / Kim Laurenson
Email: brendan.horsley@crownlaw.govt.nz / kim.lautenson@crownlaw.govt.nz

I, Joseph Eng-Hoe Teo, of Auckland, Detective, swear:

1. I swore an affidavit in this matter on 1 May 2015. Paragraph 50 of that affidavit says:

In the course of the execution of the search warrant, Detective Abbott drew to my attention a piece of paper that we considered was of interest to the investigation because of information we had already obtained.

It was seized, given the identifying number NH025 and placed with the other seized material. No further investigative steps have been taken as a result of what was seen by myself and Detective Abbott on that piece of paper.

As a result of this proceeding, on 22 October 2014 I wrote a job sheet explaining what had happened in respect of that piece of paper.


2. For clarity, I should have also said that during the search warrant I emailed a photograph of that document to Detective Constable Rachelle Smith. On 2 October 2014 Detective Constable Rachelle Smith and I deleted the email and no longer have direct access to a copy. As I indicated in my first affidavit, no steps in this investigation have been taken as a result of what Police saw on that piece of paper. Investigations in relation to the information already known to Police continue.

SWORN

at Manukau this 02nd day of June
2015

before me:


Jonelle Blaney
Deputy Registrar
Manukau District Court
~~A Solicitor of the High Court of New Zealand~~



Joseph Eng-Hoe Teo


CIY-2014-485-11344

I, David Christopher Lynch, of Auckland, Detective Inspector, swear:

1. I am a Detective Inspector in the New Zealand Police and the Counties Manukau District Manager Criminal Investigations. I have been a Police officer for twenty-one years.
2. I make this second affidavit in response to an affidavit filed in these proceedings by Wayne Leslie Stringer and second affidavit filed by Nicholas Alfred Hager.
3. Mr Stringer says in paragraph 3 of his affidavit that he was an Area Controller in Police between 2001 and 2003. For clarity, the position of Area Controller was a position held by a Commissioned Officer at the rank of Inspector. The position held by Mr Stringer was a position referred to as a 'Sub -Area Manager/Controller' at the rank of Senior Sergeant.
4. Mr Stringer last worked in an Investigative Management position in Police in the Tasman District in 1999. He has never held an investigative management position in Counties-Manukau.
5. Some of the comments that Mr Stringer makes may have been reflective of investigative standards and practices in Police at the time that he was involved in investigations. They do not have any relevance to current investigative management practices.
6. His comments in paragraph 13 suggest that in his experience serious cases were closed with lines of enquiry outstanding. An investigations manager in Police today would face serious consequences if they adopted this practice.
7. Such comments and attitudes are a graphic illustration of why Police have invested significant resource in improving investigative processes.
8. Since Mr Stringer has left Police, investigative management has been overhauled with significant changes as have investigative practices that have had to adapt to emerging technology.
9. In 2009-10 a new business model was introduced in New Zealand Police in two parts. The business model was designed to improve the 'end to end' management of investigations and case resolutions. The first part of the model

saw a comprehensive ten-step electronic 'case management' system being introduced. This was supported by initiatives such as Investigation Support Units, File Management Centres and Criminal Justice support units.

10. The second part of the business model provided for functionality on the National Intelligence Application [NIA]. NIA now provides the operating platform to manage cases.
11. The business model is designed to provide greater efficiency and accountability in investigative management as illustrated by the following excerpt from the business model *'An example of quality of case resolution includes factors like all avenues of enquiry identified, assessed and appropriately followed through to completion'*.
12. The introduction of the case management business model has significantly improved the way we manage cases and investigations in Counties-Manukau are managed in line with this business model.
13. The offence of Accessing a Computer System for Dishonest Purpose [section 249 of the Crimes Act] was introduced to the Crimes Act in 2003. It is difficult to see how Mr Stringer can give the court an expert opinion as to what is or is not an obvious and practical line of enquiry in relation to an offence that was not even in the Crimes Act when he was involved in investigations.
14. In paragraph 14 of my first affidavit I made the statement that 'a case of this nature would generally have any obvious and practical lines of enquiry to identify a suspect pursued'. This is my expectation as the District Manager of Criminal Investigations and in line with the case management business model.
15. I accept that it does not happen in all cases for various reasons. This is why I qualified the statement with the word 'generally'.
16. Mr Stringer in paragraph 8 of his affidavit suggests that my statement is 'manifestly untrue' and that Police do not have the resources to follow all open lines of enquiry in respect of this type of offending. Mr Hager also makes the commentary in paragraph 28 of his second affidavit that refers to this statement and suggests that the statement is not 'borne out'.

 262

17. From 2005 to 2014, official Police statistics record there have been 3911 recorded offences nationally under section 249 of the Crimes Act. Police have resolved 43.5% of these offences. This clearance rate suggests obvious and practical lines of inquiry are being followed through in these kinds of investigations.
18. Paragraph 30 of my first affidavit states that 'Police made several information requests in relation to the applicant as well as obtaining production orders for his bank accounts'. This statement is a factual error and the words 'Production Orders' should have read 'Information Requests'.
19. Mr Stringer's and Mr Hager's affidavit discuss the legitimacy of Police requests for banking information from Mr Hager. It was a legitimate enquiry to pursue to see if in fact Mr Hager did pay for any of the illegally obtained information. The enquiry was however two-fold in that the book itself has generated substantial revenue. That revenue was obtained indirectly from a crime punishable by more than 5 years imprisonment. This could have given rise to potential action under the proceeds of crime regime.

SWORN

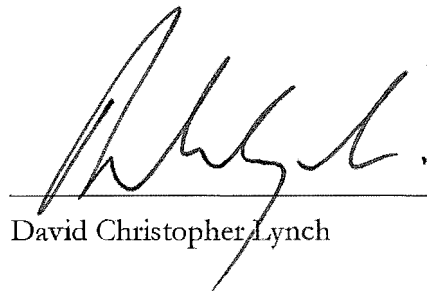
at Wellington this 25th day of
June 2015
 before me:



Varsha Budhia

Deputy Registrar
 of the High Court
 at Wellington

)
)
)
)



David Christopher Lynch

A Solicitor of the High Court of New Zealand