SERIOUS FRAUD OFFICE
TE TARI HARA TĀWARE

Version: July 2026

Senior Electronic Forensic Investigator - Club Funded Role

Team:	**Forensic Services**
Reports to:	**Principal Electronic Forensic Investigator**
Direct reports:	**None**
Indirect reports:	**None**
Delegations:	**None**
NZSIS:	**Confidential, if required**
Location:	**Auckland**
Travel:	**Occasional**

Being a Public Servant

Ka mahitahi mātou o te ratonga tūmatanui kia hei painga mō ngā tāngata o Aotearoa i āianei, ā, hei ngā rā ki tua hoki. He kawenga tino whaitake tā mātou hei tautoko i te Karauna i runga i āna hononga ki a ngāi Māori i raro i te Tiriti o Waitangi. Ka tautoko mātou i te kāwanatanga manapori. Ka whakakotahingia mātou e te wairua whakarato ki ō mātou hapori, ā, e arahina ana mātou e ngā mātāpono me ngā tikanga matua o te ratonga tūmatanui i roto i ā mātou mahi.

In the public service we work collectively to make a meaningful difference for New Zealanders now and in the future. We have an important role in supporting the Crown in its relationships with Māori under the Treaty of Waitangi. We support democratic government. We are unified by a spirit of service to our communities and guided by the core principles and values of public service in our work.

Position purpose of the Senior Electronic Forensic Investigator (Snr EFI)

- Deliver technical expertise and initiatives to operational teams to support effective investigations and prosecutions.
- Acquire, preserve, analyse, and present electronic data as evidence.
- Analyse evidence and prepare examination reports.
- Act as an electronic forensics expert witness in Court.
- Lead and support continuous improvement initiatives to strengthen the Electronic Forensic Unit's capability and effectiveness.
- Deliver mentoring, coaching, and training to support the capability development of less experienced colleagues.
- This position will predominantly support Commerce Commission casework, while also working collaboratively across other Club-funded agencies, including FMA, INZ, Serious Fraud Office (SFO) and New Zealand Customs Service.

What we do matters – Our purpose

The Serious Fraud Office (SFO) is a highly specialised government department whose purpose is to protect New Zealand's financial and economic wellbeing. We do this through our mission of disrupting and deterring serious and complex fraud through prevention, investigation, and prosecution.

How we do things – our Values

Integrity First | Ngākau tapatahi	We do what's right, with independence, fairness and courage
Sharp on Purpose | Kōpere	We act with clarity and intent, focusing our energy on what matters most
Stronger Together | He waka eke noa	We back each other, share ideas and work as one team

What you will do to contribute	As a result, we will see
Electronic forensics service delivery • Perform administrative functions including archiving and record keeping. • Maintain accurate records and ensure tasks are accurately recorded in Casper / ServiceNow. • Comply with the guidelines and procedures in the SFO EFU operations manual and supporting policies. • Process electronic data into case and evidence management systems. • Identify and propose relevant technical equipment required to optimise operational activity. • Monitor and report on current systems and processes to ensure they meet international best practice standards. • Install and manage technical equipment and recommend upgrades when required. • Contribute to business cases to acquire the latest upgrades to hardware and software.	• High quality contribution to tasks that advance the investigation strategy. • Record keeping is accurate and timely. • Compliance with guides, procedures, and policies. • Collaborative approach to work which ensures team members are aware of progress. • Effective management of timeframes and delivery of milestones. • Awareness of current international best standards. • Technical equipment is installed and managed optimally. • Effective contribution to business cases. • Well led and effective investigations and prosecutions. • Internal and external stakeholders gain enhanced understanding and technical guidance in response to their inquiries.
Collection of electronic evidence • Provide electronic forensics advice and support to operational teams in the execution of search warrants and securing electronic evidence. • Work with operational teams to acquire and filter data from electronic media that aligns with the scope of the investigation. • Collect evidence effectively to ensure the preservation and integrity of that evidence. • Troubleshoot, repair, assemble, and disassemble digital devices to access evidence.	• Collaborative approach with operational teams. • Tasks are completed to a compliant and high standard. • Devices are managed appropriately. • Evidence is acquired and secured in an optimal manner. • Business interruption is minimised. • Equipment failures are reported and documented in a timely manner. • Well led and effective investigations and prosecutions

• Follow international best practice and SFO's operating procedures in the forensic acquisition, backup, examination and reporting on electronic devices. • Ensure that there is no damage or data loss to acquired systems and devices, and absence and down time is minimised for individuals or businesses. • Report equipment failures and document the outcomes.	
Analysis of electronic evidence • Complete analysis of electronic materials and production of electronic forensics. • Work with operational teams and assist with queries. • Submit forensic analysis reports for peer review to the Principal Electronic Forensic Investigator. Ensure that technical tasks have been completed correctly and to the standard required by the Court. • Manage successful decryption of protected documents and files (to the extent possible).	• Effective and proactive identification of investigative issues. • Delivery of high-quality technical work. • Delivery of high-quality forensic analysis. • Technical tasks are completed accurately, resulting in reliable findings that uphold the truth, regardless of the details revealed. • Delivery of well-written forensic analysis reports that communicate findings with clarity and accuracy to both internal and external stakeholders.
Acting as a witness • Act as a witness in Court as a specialist and expert in computer forensics. • Continuously grow specialist knowledge to increase credibility as a witness at Court. • Understand legal boundaries and relevant case law.	• Successfully act as an expert witness. Provide expert testimony in both district and high court, articulating complex digital forensics findings in layman's terms. • EFU team members are well-prepared and skilled in court procedures and providing evidence.
Maintain capability of EFU • Provide support for service infrastructure and systems of the EFU. • Assist with the management of EFU assets. • Lead with future-proofing EFU to provide advanced electronic forensics services • Maintain and test EFU equipment, practices and techniques. • Ensure EFU leverages business efficiencies of the latest technologies and developments in combating criminal enterprises. • Mentor, coach, and train less experienced team members.	• The EFU is well managed and has the appropriate technology to undertake its functions. • EFU team members will utilise consistent and unified approaches aligned with international best practices. • The EFU is ready to respond to the latest technology developments and trends
Continuous Improvement and Best Practice • Undertake internal and external electronic forensic training.	• Investigations utilise the current best practices to analyse electronic data. • Analysis of electronic data contributes to successful investigations.

• Complete IACIS Certified Forensic Computer Examiner qualification. • Participate in research projects. • Identify opportunities for continuous improvement for the evidence management systems, processes, and knowledge. • Lead the research and development of forensic hardware and software to keep pace with rapidly changing technology needs.	• The EFU is abreast of industry advancements and technological developments in digital forensics, championing their integration into our practices for improved outcomes.
Risk Management and Compliance • Be cognisant of risks. • Risks are identified and raised with the appropriate risk owner. • Mitigate risks.	• Organisational risk is minimised, mitigated, or managed appropriately. • Reporting aligns with legal and regulatory requirements. • Reporting meets the needs of stakeholders.
Wider SFO Systems and processes • Comply with agreed systems and application access and use policies and protocols. • Enter and update data accurately and comprehensively.	• Use of systems and applications align with agreed policies and protocols. • Data is entered and updated in systems and applications accurately, comprehensively, and in a timely manner. • Systems, applications, and data risks are effectively avoided or mitigated.
Relationship Management and Stakeholders • Develop and maintain effective external relationships. • Develop and maintain effective working relationships within the SFO. • Work in a collaborative manner.	• Effective relationships that benefit the SFO and/or the wider system. • Effective relationships within the SFO.

Who you will work with to get the job done	
Internal	Forensic Services Team
	Operations Team
	Wider SFO colleagues
External	Private Sector: Victims, Witnesses, Defendant, External Panel Counsel, Defense Counsel, Contractors, Professional services firms
	Public Sector: Other law enforcement and regulatory agencies, Court staff
	Members of the public
	Investigation teams from other public sector agencies

Your competency profile	What you will bring specifically
Keys to success: • Action orientated • Manages complexity	**Experience:** • Significant experience as an electronic forensic investigator

• Customer focus	• Experience in providing electronic forensic evidence in both the district and the high courts. • Experience in providing a formal written statement for court proceedings. • Experience with e-Discovery and forensic tools such as Relativity, FTK Imager, X-Ways, Axiom, Intella, Forensic Explorer, as well as mobile forensic tools such as Cellebrite. **Skills:** • Proven technical expertise in electronic forensic tools and methodology • In-depth knowledge of e-Discovery and forensic tools: Cellebrite, Paladin, Axiom, Forensic Explorer, Intella, and others • In-Depth knowledge of SQLite Databases • Social media and cloud investigations • Desktop, laptop, and mobile device forensic analysis • Ability to meet deadlines in an environment of competing/conflicting priorities • Ability to work independently and under direction. • Effective influencing skills • Effective communication skills • In-depth understanding of the wider agency operating and legal/technical environments • Ability to develop and deliver training in the electronic forensic field • Strong problem solving and decision-making capabilities **Other requirements:** • Tertiary qualification in a related field • Industry standard certification(s) such as: CFCE, EnCE, ICMDE, CCPA, CCME (Preferable) • Forensic tool and script development • Obtain and maintain required advanced digital examiner/forensic certifications through an international association (IACIS) • Ability to maintain and hold qualifications with the Electronic Forensic Unit training framework • Ability to continue learning in the field of electronic forensics • Ability to obtain and maintain any required Security Clearances • Holds an unrestricted and full drivers licence • Demonstrated knowledge of the Serious Fraud Office Act 1990

	• Ideally, knowledge of criminal legislation, such as the Crimes Act, Criminal Procedures Act, Evidence Act, Search and Surveillance Act 2012. • A growth mindset