Michael Roberts

Recent Career Highlights:

2020: Solved what FBI Special Agent described as “an unsolvable case” by defeating VPN and ProtonMail obfuscation attempts by a vicious pedophile, and inadvertently uncovered an international ring of at least four offenders.

2013: Michael was engaged as a civilian agent in a foundering, multi-agency, 2-month national manhunt for a murder fugitive. He located the suspect in just 73 minutes leading to his arrest by U.S. Marshals.

Coordination of digital forensics and counter-hacking training for the U.S. Air Force, Marines, Army & Navy. Other clients include NATO, Australian DoD and the United Nations, to name just a few.

Consulted for private and law enforcement clients. Clients range from bullied school children, celebrities, prosecutors, CEOs and Heads-of-State.

2012: Secured the release of a man, who had been held in jail for 12 days, for allegedly sending electronic death threats. As part of a sting operation, Michael was able to prove that the death threats were actually conveyed by the so-called victim in order to frame the client.

Michael was described by the investigative journalist as: ***“… an absolute secret weapon for any serious reporter.”***

EXPERIENCE

Rexxfield®

Private Investigator & Litigation Support Consultant 2008 to Present

Responsible for cyber investigations in criminal and civil cases. Litigation support, preparation of technical subpoenas and warrants, preparation of depositions and interrogatories, expert witness testimony pertaining to electronic evidence and artifacts. Preparing presentations - “publishing to the jury” to demystify technical evidence.

IT Security & Counter Hacking Education Facilitation 2003-2008

Responsible for identifying gaps in contemporary IT Security education, certifications and vulnerability best practices. Facilitated high level counter-hacking and digital forensic courses for Military, Government and regulated industries throughout Australasia, Europe, Africa and the Americas. Secured sole-source USAF contracts for “Red Team” hacker training for various Air Force bases globally.

Contract IT Instructor Broker - USA 1996 - 2003

Developed a network of over 900 instructors globally, primarily in the Information Technology arena. Clients were primarily large commercial training organizations requiring contract human resources for short-term training needs. The business began in his Chicago basement, with a handful of instructors, to a thriving business with over $7M in revenue.

Entrepreneur 1986-1996

Various entrepreneurial pursuits

Australian Telecommunications Commission 1985-1986

Investigator – Secret Clearance. Michael worked briefly for the government-owned company "Telecom" and was later assigned to a security department that collaborated with state and federal law enforcement agencies to investigate and monitor illegal activities using Telecommunications infrastructure. Security clearance given by the Australian Security and Intelligence Organization (ASIO). Youngest officer to be appointed to the position.

michael@rexxfield.com

Brief Biography

Michael is a seasoned professional in the field of digital forensics and cybersecurity, began his journey in Australia, where, in the mid-80s, he was recruited as the youngest investigator with the Australian Telecommunications commission. Subsequently, he has worked as a licensed private investigator in Australia, The United States and Europe.

Michael worked with law enforcement agencies around the world, including the US Marshals, the Department of Homeland Security, the FBI, and police from Switzerland to Australia. His expertise proved invaluable in criminal investigations, and led to convictions, particularly in identifying anonymous internet users and assisting in arrests and convictions. Michael's work has also proven the innocence, and release from jail, of falsely accused cyber criminals, in three separate cases.

In 2003, Michael founded Mile2.com, an IT security training company that quickly became a benchmark in the industry. Mile2's certifications in counter-hacking and digital forensics were recognized by various organizations including the US Air Force, United Nations, Australian Defense Force Signals Directorate, and many law enforcement agencies. Under Michael's leadership, Mile2 was awarded prestigious contracts and played a significant role in the training of various military and law enforcement personnel.

After selling Mile2 in 2008, Michael shifted his focus to Rexxfield, a digital forensics investigation business unit that further solidified his status as an industry leader. His experience in identifying internet users engaging in illegal online activities grew extensively during this time.

Michael also founded Picdo, Inc., a US 501(c)(3) charity with the mission to reduce the burden on government by teaching law enforcement agents best practices in cybercrime investigations.

Over the years, Michael has appeared as an expert witness in civil litigation cases and as a general witness in criminal cases in the United Kingdom, the United States, and Australia. His extensive experience in unmasking bad actors using communication technologies to commit crimes has made him an indispensable resource in the field of digital forensics and cybersecurity.

Case 1: Apprehension of Murder Fugitive in just 73 minutes after a two-month manhunt - 2013

The Brief — Michael assisted a joint task force of U.S Marshals and the Maryland State Police Force in the 2-month manhunt for a fugitive, who had been on the run in connection with the murder of a 26-year-old man, on June 21, 2013.

The Outcome —

1. Michael developed a pretext for a sting operation and then, after approval from law enforcement, conveyed a message to one of the suspect's family members. The message had one of Michael's proprietary tactical tripwire payloads attached thereto.
2. The tripwire detected many electronic signals, caused by the fugitive hiding behind anonymous servers to obfuscate his location.
3. Over the next few hours, Michael continued to work with the task force to circumvent the fugitive's attempts to obfuscate his activities and location.
4. As a result of the digital artifacts and intelligence collected by Michael, within a few hours, the team identified a cell phone number. The SIM card that the fugitive had was disposable and didn't reconnect to the cell-tower network, so it was impossible to locate them through triangulation.It

michael@rexxfield.com

appeared that the fugitive had purchased the SIM card to use once for an emergency and thereafter destroyed it.

5. Upon consulting with Michael, U.S. Marshals obtained a warrant and were able to obtain the Unique Device Identifier [UDID] that was associated with the one-time-use SIM card. A few days later the same UDID connected again to the national cellular infrastructure, but in association with a new disposable SIM card. The US Marshals were then able to triangulate the physical location of the fugitive who was then arrested interstate, and remanded for trial.

Case 2: 2020 — Solved Pedophile Case That FBI Declared "Unsolvable"

The Brief — A vicious pedophile had been tormenting the grieving mother of a small child who had been abducted, raped and murdered. He had been sending extremely disturbing fantasies about what he would have done if he were the murderer.

The Outcome — Michael was able to defeat the identity obfuscation safeguards employed to geographically locate the pedophile and capture enough evidence to allow police to positively identify the offender and at least three members of his international ring.

Case 3: State Police Service, Fraud and Corporate Crime Group (Computer Crime Investigation Unit)

The Brief —

A threat was made against an Australian state police service that included an attack against its online resources and the publishing of officers' database information. This threat, if carried out, would have cost untold tens, if not hundreds of thousands of dollars; as well as severely compromising reputation, confidentiality, safety and operational standing of active members.

Michael's team's brief was to use the limited intelligence the Police Service had available to determine if it were possible to build a better profile and identify threat originators from anonymous personas and online accounts he had created. The Police Service had made no headway in more than 10 days.

The Outcome — Michael's team was able to:

1. Positively identify operational personas and true identities of the key participants, resolve network infrastructure, geolocation and other identifying details. The lead hacker was identified within three hours.

2. Map additional communications channels and methodologies used by associated personas.

3. Identify a *nest of HACTivists* in the form of a group of 1000+ friends within an obscure social networking platform, used for covert communications and private messaging, outside of mainstream and highly scrutinized social networking platforms. This discovery was a mother lode of intelligence.

4. Recover deleted and private communications and collect public communications exchanged by the key perpetrator.

5. Make a simplified guide for Police Service staff that outlines the necessary investigation steps, removing any extra information. In doing so a sworn officer was able to duplicate the intelligence gathering and evidence preservation steps required to positively identify the key perpetrator and inexorably link all relevant communications to that individual. This allows the officer to testify in court to get warrants and testify before the jury without requiring Michael to disclose his methods or involvement publicly.

Case 4: Diplomat Espionage Vulnerability Eliminated

The Brief — A Diplomat (BB4/BB3 officer) from a Commonwealth nation lost control of some compromising photographs. It was suspected that her former partner, working for her nation's defense intelligence community, began publishing images anonymously on gossip and file sharing websites. The risks of allowing the threat to persist included the personal cost of loss of face, loss of employment and potentially compromising national security through extortion.

The Outcome — Michael and his team were able to identify:

1. all offending digital publically available artifacts thus, enabling their removal.

2. the antagonist's location and various digital artifacts.

We stopped the person who was causing problems. They are not bothering or contacting the client anymore.

Case 5: Celebrity Trolling and Tortious Interference by Competitors

The Brief — An American celebrity, sports-business person came under an organized Internet defamation and smear campaign by true name, anonymous and pseudonymous individuals. The campaign against the person was falsely presented as a protest by the public, with mostly untrue claims.

Whereas, what appeared to be public outrage was in fact a carefully crafted conspiracy consisting of one protagonist in association with ten or fewer lesser antagonists, each suspected of using multiple alter egos in what is called "astroturfing". This handful of conspirators was then able to mobilize scores if not hundreds of individuals involved in the specialty sport into adopting the false allegations as their own opinions and causing a wildfire of uncontrollable negative sentiment by the viral crowd.

The personal cost of this concerted effort against the client was estimated to be in the millions of dollars.

The Outcome — The small team, lead by Michael, was able to:

1. Positively identify the key individuals responsible for publishing and administering cornerstone websites despite:

    a. the use of proxy services and IP addresses.

b. anonymous domain registrations through a Panamanian company using cash/money order transactions.

2. Investigate, identify and monitor the plethora of usernames over multiple websites, forums and social networking pages and:

   a. isolate smaller groups/cells of organized conspirators.

   b. positively identify the individuals and addresses behind some of these usernames.

   c. Advise the client on how to prevent more damage and fix the damage already done.

Michael's team helped the client gather evidence that led to the suspension of the main website(s) used for the attack.In doing so disrupting many weeks of the conspirators' search engine optimization, back-linking, and information sharing through social media.

Case 6: Wrongly Accused Released From Jail - 3 cases.

The Brief — This was a pro bono case. A North Carolina man was arrested for allegedly sending death threats electronically to his estranged wife. The personal cost was a loss of freedom through incarceration and loss of child custody, income, assets and reputation.

The Outcome — Michael was able to prove that the communications originated from the alleged victim who was setting up the man to gain an advantage in child custody proceedings. Michael submitted evidence and supporting affidavit to prosecutors. The man was then released after 12 nights in county jail. Michael also vindicated two women, in unrelated cases, in 2023 in similar circumstances.

Case 7: David Jones Fraudulent Takeover Bid & Stock Manipulation

The Brief — To identify the individual linked to a multi-billion takeover bid of one of Australia's largest department stores; the case had been shrouded in mystery and was being heavily scrutinized by skeptics.

THE AGE
theage.com.au

DAVID JONES

Fairfax Media Journalist Rachel Wells' personal account of this case is below:

"I recently contacted Michael to help me on one of the biggest breaking business news stories in Australia's recent history. The brief was to help identify the individual linked to a multi-billion takeover bid for one of Australia's largest department stores, which had been shrouded in mystery and skeptics, and had sent the local stock market into a frenzy. All I had was an internet address, linked to a so-called 'business'. Within minutes, Michael rang with a name – a name which no other news media outlet in the country had. And within hours I had a 22 page report outlining what appeared to be a detailed history of the corporate internet activities of one 'John Edgar' of Newcastle, in the United Kingdom. This information allowed me to gain a great insight into the background and legitimacy of this individual and also the crucial information to enable me to attempt to make contact with him and any so-called business associates.

michael@rexxfield.com

In a follow-up phone call, Michael was also able to give me his expert opinion on the credibility of this person's business dealings, based on his expeditious but utterly thorough social forensics. His verdict:

> *'my gut feel is that this gentleman might be all feathers and no meat; there doesn't seem to be much in the way of human gatekeepers between him and the outside world. He uses free Yahoo e-mail addresses, and does not make much effort to obfuscate his online activities.'*

Not only did his 'gut feel' prove spot on, but Michael's work allowed us to beat our competitors to the punch – with by far the day's most compelling, colourful and insightful story on the mystery bidder.

Michael can be relied upon to respond to such requests with remarkable promptness and his work has proven not only thorough and comprehensive but accurate and efficacious. His skills have not only enabled me to break stories but to obtain background and information that could take days, if not weeks or months, using traditional boots on the ground journalism. In fact, he has the ability to obtain information that most journalists could never obtain. He is an absolute secret weapon for any serious reporter."

Case 8: The Dunkin' Donuts Matter - Extortion and Racketeering

The Brief — A US-based insurance adjuster discovered a website (his-business-name-scam.com) which was established for the sole purpose of hijacking search engine results for his business and repulsing prospective customers. The client was reasonably informed on e-commerce issues and discovered eleven additional victims.

The group of victims engaged one of Michael' few competitors, who failed to produce any results after several months. The group then engaged Michael to assume responsibility.

The Outcome — Within 36 hours Michael was able to identify the extortionist (who was on parole), the client was then able to obtain video footage of the perpetrator in the act while connected to a public Wi-Fi at a *Dunkin Donuts* franchise.

Upon presenting the evidence to the perpetrator, Michael was able to leverage him for control of the attack domains and caused the demeaning materials to be deleted from the Internet.

Case 9: Global Smear Campaign Extortion Racket

The Brief — Michael completed a seven-month digital and social forensics investigation that uncovered a massive organized crime and murder racket, that targeted wealthy European entrepreneurs with threats of Internet smear campaigns if they did not submit to the criminals' extortion demands.

The Outcome — Over the course of the investigation, Michael was able to identify the principals behind the racket. They were located in Eastern Germany, Switzerland, British Virgin Islands, Republic of Seychelles and elsewhere. The threat to the client was eliminated through disclosure of the participants; the matter was then referred to Interpol.

Case 10: Celebrity Smear Campaign & Extortion

The Brief — Michael and Anna conducted a digital and social forensics investigation for the co-founder of the Global Craft Beer chain "Brewdog".

The Outcome — Rexxfield's work resulted in the criminal conviction of Ms. Emili Ziem, and a court ordered restitution of equivalent to USD 675,000. This case made world headlines and can be reviewed here.

Counter Extortion and Cyber-Crime Investigations Explained

When approaching complex cyber-crimes, it is important to understand the perpetrator's modus operandi. In most cases, things are not what they seem. These criminals are experts in subterfuge, using red-herring tactics to disguise their true intentions. If hasty countermeasures are implemented, it alerts the offender to the scrutiny and can give the victims a false sense of security thinking that the threat has been eliminated, without knowing the extent of the vulnerabilities.

Michael uses critical thinking and deductive reasoning skills, developed over many years of "getting inside the criminal mind"...

Positive identification of criminals using the techniques outlined above, where appropriate, with the addition of the following:

- Identify geographic nexus of crime
- Foot-printing the criminal's social, technical, financial and operational networks
- Evidence and artifact collection and preservation
- Evidence chain of custody management
- Law enforcement liaison (for smaller branches lacking digital investigative staff)
- Litigation support (criminal and civil cases):
    - Assisting lawyers in drafting complaints/statements of claim
    - Drafting subpoena and discovery requests
    - Identifying witnesses
    - Drafting interrogatory questions for suspects
    - Expert testimony

Case Preparation for Submission to Law Enforcement and Lawyers

All of the above elements can be merged to build a preliminary case file for submission to law enforcement for "parallel reconstruction" of my team's work in instances of criminal acts, or to lawyers for civil action. In criminal cases, law enforcement investigators will be more likely to act due to the value-added nature and for being "without excuse" due to the well-developed prima facie evidence, and the ability to determine work load required and likely case outcome from the outset.