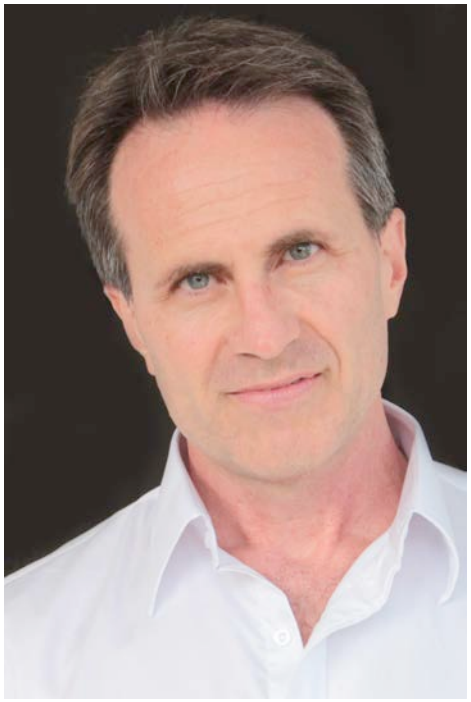
+1-408-916-5977 |forensics@rexxfield.com



Mike Roberts

Mike is a Licensed Private Investigator and a civil/criminal litigation support specialist.

Recent Career Highlights

In 2013, Mike was engaged as a civilian agent in a floundering, 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 and Navy. Other clients include NATO, Australian DoD and the United Nations, to name just a few.

Consulting for private and law enforcement clients ranging from bullied school children, celebrities, prosecutors, CEOs and Heads-of-State.

In 2012 Mike 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 Mike was able to prove that the death threats were actually conveyed by the so-called victim in order to frame the client.

In 2012, Mike gave Fairfax Media's "The Age" a scoop, when he positively identified the man behind the fraudulent stock manipulation/takeover bid for David Jones Department Stores.

Mike was described by the investigative journalist as: ***"... an absolute secret weapon for any serious reporter."***

EXPERIENCE

Current Case updates are published here [LINK]

Private Investigator & Litigation Support Consultant - 2008 to Present

Responsible for factual 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.

Ideas and the Investor Ltd – Joint Venture Facilitator 1995-1996

"Ideas and the Investor" was a private company fully funded by the Australian Government. I&A was contracted to provide facilitation services between domestic and foreign investors and Australian inventors and innovators. In the short life of the program, Mike was responsible for more funding and joint ventures than the other six states combined.

Entrepreneur 1986-1995

Various entrepreneurial pursuits

Australian Telecommunications Commission – Investigator 1986-1994

Investigator – Secret Clearance. After brief clerical employment with the Government owned "Telecom" company, Mike was seconded to a security department that investigated and monitored illegal activities using the Telecommunications infrastructure in cooperation with state and federal law enforcement agencies. Secret clearance given by the Australian Security and Intelligence Organization (ASIO). Youngest officer to be appointed to the position.

University of Central Queensland Rockhampton Australia 1993

Bachelor of Business (incomplete)

Achievements: Set all-time school record for highest mark on major marketing assignment – "Comprehensive Business Plan"

Capability Overview Through Case Study Examples

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

The Brief -- Mike 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. Mike 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 Mike's proprietary tactical tripwire payloads attached thereto.
2. Subsequently, the tripwire transmitted numerous electronic footprints, including incidents triggered by the fugitive from behind anonymous proxy servers, presumably in an attempt to disguise his location. Over the next few hours Mike continued to work with the task force to circumvent the fugitive's attempts to obfuscate his activities and location.
3. As a result of the digital artifacts and intelligence collected by Mike, within a few hours the team identified a cell phone number. It was allocated to a disposable SIM card in the possession of the fugitive, but it did not reconnect to the cell-tower network after Mike first discovered it — ergo triangulation was impossible. It appeared that the fugitive had purchased the SIM card to use once for an emergency and thereafter destroyed it.
4. Upon consulting with Mike, 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: 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.

Mike'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 – Mike'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 and rebuild an archive of communications conducted and exchanged by the key perpetrator, in effect recovering deleted communications, retrieving conversations, believed to have been private, and collecting existing public communications.

5. Create a walk-through "cheat sheet" for Police Service personnel which essentially reduced Mike's work product to only the essential investigation steps by eliminating the superfluous elements. 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. Thus enabling the officer to testify under oath as necessary to obtain warrants, and eventually testify before the jury, rather than requiring Mike to go public with methods and involvement.

Case 3: Diplomat Espionage Vulnerability Eliminated

The Brief -- 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 – Mike 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.

The culmination of our efforts resulted in the perpetrator ceasing all malicious activities; the individual is no longer stalking, publishing, threatening or communicating with the client at that point in time.

Case 4: 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 smear campaign was framed as a grassroots public outcry against the individual with factual allegations supported, for the most part, only by logical fallacies in the form of ad hominem, straw man and other common fallacious arguments.

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 Mike 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 the best strategic and tactical go forward actions to mitigate further damage and remedy, inasmuch as it was possible, the damage already inflicted.

As a result of Mike's team's engagement in this case, the client was able to leverage the evidence gathered to bring about the immediate suspension of the primary website(s) used in the attack and in doing so disrupting many weeks of the conspirators' search engine optimization, back linking, and information sharing through social media.

Case 5: Wrongly Accused Released From Jail

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 loss of freedom through incarceration and loss of child custody, income, assets and reputation.

The Outcome -- Mike 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. Mike submitted evidence and supporting affidavit to prosecutors. The man was then released after 12 nights in a county jail.

Case 6: 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 Mike 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, Mike 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.

In a follow-up phone call, Mike 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 Mike'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.

Mike 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 7: 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 Mike' few competitors, who failed to produce any results after several months. The group then engaged Mike to assume responsibility.

The Outcome -- Within 36 hours Mike was able to positively 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, Mike was able to leverage him for control of the attack domains, and caused the demeaning materials to be deleted from the Internet.

Case 8: Global Smear Campaign Extortion Racket

The Brief -- Mike 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, Mike 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.

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.

Mike 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 further action in instances of criminal acts, or to lawyers for civil action. In doing so for the former, 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.

+1-408-916-5977 | forensics@rexxfield.com