

## Opinion of Mottershead report submitted to the USCF

David Ulevitch  
December 17, 2007

### Introduction

On or around October 5<sup>th</sup>, 2007 I was contacted by a reporter from The New York Times to provide some background information and expert advice regarding an article he was preparing that was ultimately published on October 8<sup>th</sup>, 2007 as “Chess Group Officials Accused of Using Internet to Hurt Rivals.”

My background in Internet Security spans almost 10 years during which time I have worked for Internet Service Providers, Universities and businesses, as well as run a number of my own. I am considered an expert security practitioner. I have also had extensive experience working with various national and international law enforcement organizations in a consulting capacity.

My intention in this letter is to provide a perspective on the techniques used by Brian Mottershead in his report to the USCF. This report should be considered a preliminary release. My analysis of the Mottershead report is complete but I expect I may revise this report to add clarification as needed based on feedback. I am happy to do so. For the record, I have never been a member of the USCF, I do not know any of the parties involved personally and I have no known vested interest in this issue other than to help provide an honest and accurate perspective of the Mottershead report.

My initial reaction to the Mottershead report was an appreciation for the detailed level of evidence and chronology of research that is provided. Typically, when doing computer forensics, it is common to attempt to tie what you know with what you don't know. This is exactly what Mr. Mottershead did, many times in his report. When you can correlate the known with the unknown as many times as Mr. Mottershead did in his report you create a crystal clear depiction of activity and actions that can stand up on their own. Furthermore, subpoenaing billing records from both ISPs and credit card companies can extend this chain of evidence by directly linking an IP address to the ISP and to an individual paying the bills. It is my opinion, and as I'll show from some examples below, I find this step unnecessary.

### Excerpt 1:

*Since the IP addresses of Usenet posters are public information, and in the USCF web logs and database I had information as to the IP addresses of USCF members accessing the forums, it seemed likely that I would be able to identify the USCF member account that was being used by the Fake Sam Sloan to mis-appropriate USCF Issues forum posts for his posts on Usenet.*

Mr. Mottershead is accurate in his explanation of what he wants to accomplish. He is correct in stating that Usenet postings are tied to an IP address. The IP address recorded in these types of posts cannot be spoofed. He also knows the login name for the parties involved on the internal USCF member forums and their posting IP address. This too cannot be spoofed. By connecting what he knows, with what is publicly archived by Google (and others) he can create a direct correlation.

Mr. Mottershead shows clearly through examples (a) (b) and (c) that the IP addresses posting to Usenet and the physical location of Mr. Truong are directly connected. He also connects that to the known forum identity of Mr. Truong. To be clear, three facts have just been established:

- 1) The Usenet postings are being posted from the same physical location that Mr. Truong is believed to be in at the time of the posting.
- 2) The IP addresses on the USCF forums, which are tied to the username used by Mr. Truong, are also being made from the same physical location that Mr. Truong is believed to be in at the time of the posting.

- 3) In nearly all cases, the IP addresses tied to the Usenet postings are the same as the USCF forum posting IP addresses.

**What about someone spoofing all of this?**

Often, people say that they were spoofed or that their IP address was hijacked. While it is possible that someone can sometimes change his or her posting name on a forum or a message board to look like that of another user (consider “Bob” and “Bob ”), the IP address cannot be spoofed.

Let me explain why an IP address cannot be spoofed. First, for a post to Usenet to happen it requires that there exist, at the most rudimentary level, what is known as the “TCP Three-way handshake.” This handshake is when two machines on the Internet wish to establish a connection. In layman terms, in order for that handshake to occur the sender extends a signal to the recipient saying, “Here I am, let’s talk.” The recipient replies to the sender saying, “Okay, go ahead.” Finally the sender acknowledges that they have shaken hands. In order for this back and forth to occur, which is required for any Usenet posting to happen, the IP addresses cannot be spoofed or the handshake would never complete.

**What if someone was following around Mr. Truong?**

This is highly unlikely given the preponderance of evidence, however it can be easily proven false by correlating ISP billing records to IP address leases. ISPs maintain a timestamped log of what customer is assigned what IP address at what time.

**What if someone used Mr. Truong’s name on the ISP bill?**

Again, as we enter areas of criminal identity fraud, it is unlikely someone would go to these measures to cover their tracks, however, this can be verified by contacting the credit card issuer and verifying it is a legitimate account in good standing and correlating purchases on the card with other known valid purchases.

**Conclusion**

The report provides over a dozen different data points from IP addresses to locations to user-agents and more that all lead to a single conclusion with an overwhelming amount of evidence. The methods used by Mr. Mottershead were appropriate and accurate. There is also far too much public evidence for it to have been tampered with. Even if the forum logs were compromised, that doesn’t change the Usenet postings and the surrounding evidence, which could not have been altered.

It’s my belief that this report has been compiled in an accurate way that deserves recognition for its comprehensive depth and detail.

Thank you,  
David Ulevitch