IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF OHIO

EASTERN DIVISION

UNITED STATES OF AMERICA,	)	CASE NO.: 1:15-CR-00275
	)	
Plaintiff,	)	JUDGE DAN AARON POLSTER
	)	
v.	)	
	)	
JOHN CLEMENTS,	)	GOVERNMENT'S MOTION FOR 30-DAY EXTENSION FOR INDEPENDENT TESTING BY CIGITAL, INC.
	)	
Defendant.	)	

Now comes the United States of America, through its counsel, Carole S. Rendon, Acting United States Attorney, and Brian McDonough, Assistant United States Attorney, and respectfully moves this Court for a 30-day extension for independent expert Cigital, Inc. to test the software in this case. Cigital should have the independent testing completed within 30 days. Additional information is in the attached memorandum.

Respectfully submitted,

CAROLE S. RENDON
United States Attorney

By: /s/ Brian M. McDonough

Brian M. McDonough (OH: 0072954)
Assistant United States Attorney
United States Court House
801 West Superior Avenue, Suite 400
Cleveland, OH 44113
(216) 622-3965
(216) 522-2403 (facsimile)
Brian.McDonough@usdoj.gov

MEMORANDUM

I. Introduction

After reviewing Defendant's Motion to Suppress or, in the Alternative, Motion to Reconsider Defendant's Motion to Compel Discovery (Doc #: [22]), the Court held a teleconference on March 17, 2016, with Assistant United States Attorney Brian McDonough for the government and Attorney Eric Nemechek for Defendant to discuss the Motion. As a result, the parties agreed to confer and agree upon an independent person/entity to test the Shareaza LE software used in this case to determine if the software allows the user to access any part of a computer that is not otherwise publicly available -- and to do so within 30 days from today. As such, the Court denied the motion to suppress as premature.

From March 17th through March 24th counsel have researched independent experts/entities to perform the software testing in this case. On March 24th, defense counsel suggested Robert Young of Johnson-Laird, Inc. See Exhibit A. On Friday, March 25th, government counsel emailed defense counsel and wrote that the undersigned would research Mr. Young and update defense counsel. See Exhibit B. On March 28th, the undersigned telephoned defense counsel and informed him that Mr. Young's credibility had been called in to question in U.S. v. Lofthouse, where his testimony had been stricken. See Exhibit B. The government suggested Cigital, Inc. ("Cigital") as an independent expert. See Exhibit B. On the March 28th, government counsel emailed defense counsel with Cigital's website: http: www.cigital.com. To date, defense counsel has not objected to Cigital as the independent expert. Eighteen days later, on Friday, April 15th, defense counsel suggested that as an alternative to Robert Young, Dr. Marcus Rogers be selected as an independent expert. See Exhibit C. Given that the defense has

never objected to Cigital, the government proposes that Cigital perform the independent testing in this case under the analysis listed below.

II. Cigital's Independent Testing of the Law Enforcement Software Used in This Case

Cigital has its principal place of business at 21351 Ridgetop Circle, Suite 400, Dulles, Virginia, 20166. Cigital can review the software source code and related scripts originally based on the LimeWire peer-to-peer networking protocols to automate searching for users distributing child pornography on the Gnutella network. Cigital will review any changes made to LimeWire by the law enforcement software to determine whether it simply queries/gathers publicly known information, or whether it exploits vulnerabilities in the LimeWire based source code or supporting protocols to access Gnutella clients to gain access to information that may not be normally available.

Cigital proposes the following analysis:

- Obtain LimeWire source code from a public repository, build it and ensure that it installs and runs. Document default file sharing settings in LimeWire.
- Obtain source code for the law enforcement software based on LimeWire, build it and ensure that it installs and runs.
- Determine which LimeWire files were added/deleted/modified by the law enforcement software using the following approaches:
    - Perform directory listings to determine which files have been added or deleted.
    - Generate a cryptographic hash of each file in both source trees. Determine which files have changed by looking at which files have different cryptographic hashes in the two source trees.

- For files that exist in both source trees, perform a 'diff' on both versions of the file to determine which ones have been modified. This will provide yet another mechanism to determine if any files have changed, and will also provide details about the exact changes that have been made by the law enforcement software.

- Analyze the list of changes gathered using the above techniques and manually review the relevant code to determine if or how LimeWire's functionality has been altered.
- If, after performing the above steps, it appears that the law enforcement software only looks for normal information, Cigital will run the version that was built earlier and ensure that it is capable of finding the types of information and/or files that the law enforcement software claims its tool can find (e.g. images in default directories). This is done to validate that law enforcement software provided source code executes queries and processes responses as expected.
- Run the law enforcement software, as well as unmodified LimeWire (the versions built earlier), and analyze network traffic generated by the two pieces of software. This is done to ensure that law enforcement software is not sending any traffic that could perform operations that LimeWire would never perform.

Using the above techniques, Cigital will attempt to determine whether the following assertions are true:

- The law enforcement software does not exploit a vulnerability in any software.
- The law enforcement software does not misuse the protocols on the Gnutella network to do things that it was not intended to do.

- The law enforcement software does not change any configuration options in other users' software to extract information that would normally not be publicly available (e.g. it does not make other users' software share private parts of their filesystems).

III. Conclusion

For the reasons stated above, the government moves this Court for a 30-day extension for independent expert Cigital, Inc. to test the law enforcement software in this case.

CERTIFICATE OF SERVICE

I hereby certify that on this 18th day of April 2016, a copy of the foregoing document was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. All other parties will be served by regular U.S. Mail. Parties may access this filing through the Court's system.

/s/ Brian M. McDonough
Brian M. McDonough
Assistant U.S. Attorney