EXHIBIT A

The Honorable Robert J. Bryan

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. DAVID TIPPENS, Defendant.	NO. CR16-5110 RJB **DECLARATION OF JOHN POWERS**

I, John Powers, declare as follows:

1. I am a Forensic Examiner with the FBI Computer Analysis and Response Team (CART) and have been for approximately five years. Before joining the FBI, I was a computer forensics volunteer at the Lafayette Police Department (Indiana) and have a B.S. degree in Computer and Information Technology from Purdue University. A copy of my CV listing my full qualifications is attached to this declaration.

2. I am the computer forensic examiner assigned to conduct a forensic examination of digital devices seized during the search of Defendant David Tippens's residence on February 11, 2016.

3. I have also reviewed the declaration of Professor Matthew Miller filed as Exhibit A to Defendant's Second Motion to Suppress (Dkt 127).

4. Although Professor Miller is correct that there are differences in how the TorBrowser and less security oriented internet browsers operating over the open internet handle web-based content, several points require clarification.

5. While TorBrowser is designed with security and privacy features intended to reduce the traceability of a user's web activity, these features are not infallible and still leave a forensic trail.

6. After all, in order for a user to view web content, that content must necessarily be downloaded to the user's computer. For example, if a computer user visits www.cnn.com using the TorBrowser, the webpage content, including images, would need to be downloaded to the user's computer. Otherwise, the user would not be able to view the page or access any of the content offered. The same would be true when visiting a Tor hidden service, such as Playpen, using the TorBrowser.

7. To be sure, TorBrowser is designed to store that content in a manner that makes it very difficult for someone to access that content in any meaningful or useable form in the future. However, the content is nevertheless viewable and therefore downloaded at least while the user is viewing it.

8. As a result and notwithstanding TorBrowser's security features, traces of that content often remain and may be recovered through a subsequent forensic examination of the computer.

9. Professor Miller discusses, for instance, TorBrowser's ability to avoid storing data such as web content that an ordinary web browser would place in a temporary cache file on the computer's local hard drive. He correctly notes that TorBrowser may instead store this information in Random Access Memory (RAM), where it is impractical or even impossible for a normal user using normal software to later access that information. In addition, because RAM is likely to be overwritten with some frequency, this information, even if it were accessible, is likely not to persist for a long period. In contrast, information saved to a hard drive may persist for a much longer period as the available space is far greater.

10. Professor Miller fails to account for the fact that TorBrowser is not the final or sole arbiter of what information may be written to a computer's hard drive. Indeed, there are several system processes that may cause a computer to write the contents of RAM to its hard drive. The most common of these are virtual memory (also called "swap files" or "page files") and hibernation files.

11. With virtual memory, the computer essentially treats part of the hard drive as an extension of RAM. Contents of RAM are written to the hard drive and then traded back and forth between the hard drive and the actual RAM as needed. In effect, this process allows a computer to behave as if there is more available RAM than physically exists.

12. Hibernation files are used when a computer goes into hibernation mode. This is a mode that allows the computer to be shut down and then later restored to its earlier state. Since, as Professor Miller correctly notes, the contents of RAM are volatile—*i.e.*, they disappear when power is lost—its contents must be written to persistent memory, such as the hard drive, to ensure that the computer can be restored to its pre-hibernation state.

13. Because TorBrowser cannot control the virtual memory or hibernation process, information it places in RAM in an attempt to make it less accessible could nevertheless be recovered at a later date under certain circumstances. This could lead, for example, to the recovery of information such as URLs (the human readable address of a website) that a user visited using TorBrowser.

14. Use of TorBrowser leaves other artifacts that may shed light a computer user's activities. For example, it may be possible through forensic analysis to determine the first or last time TorBrowser was started on a computer and how many times the program was started.

15. And like with any traditional web browser, TorBrowser allows users to save content with relative ease. For example, someone using TorBrowser to view a webpage

can save an image, video, or other webpage content with a few mouse clicks. The process is no different from that used in Internet Explorer or Google Chrome.

16. Indeed, during my work on this case, I noted that there are files related to TorBrowser on Defendant's Dell laptop. My analysis also revealed that at one point, there were folders on that laptop entitled "CP Link List for TorBrowser" and "Playpen CP Forum." These items no longer exists on the computer, and their contents are therefore unknown, however.

17. These observations are noteworthy in at least two respects. First, they provide real-world examples of the types of forensic artifacts that may remain on a computer notwithstanding the unique security features TorBrowser offers. Second, I noted these items despite the fact analyzing Defendant's TorBrowser habits was not one of the primary aspects of my forensic work to date.

EXECUTED: February 6, 2017.

John Powers

John Powers
ITS-FE, FBI

CURRICULUM VITAE

FBI Expert Witness

John B. Powers

Federal Bureau of Investigation
Computer Analysis Response Team
1110 3rd Ave
Seattle, WA 98101
PHONE: (206) 287-3612

PROFESSIONAL EXPERIENCE

Feb 2012 - present

Information Technology Specialist- Forensic Examiner
Seattle Division
Federal Bureau of Investigation

Examine digital evidence under a documented quality assurance program that includes annual proficiency testing, technical/peer and administrative reviews and adherence to standard operating procedures. Assist in the planning, coordination and execution of search warrants involving multiple federal and local law enforcement agencies. Assist investigators and attorneys in technical matters pertaining to digital evidence.

Mar 2014- present

Evidence Response Team Member
Seattle Division
Federal Bureau of Investigation

Preserve, document, and collect evidence from crime scenes. Conduct training in evidence recovery techniques.

Jan 2008 – Feb 2012

Computer Forensic Volunteer
Lafayette Police Department
Lafayette, Indiana

Image and process digital evidence, conduct analysis of digital evidence, assist in writing reports, assist at search sites, assist in instruction of patrol officers on cell phone examinations, testify in court.

EDUCATION

B.S. Computer and Information Technology with a minor in Forensic Science – Purdue University

B.A. History – Purdue University

FORENSIC EXAMINATION

Conducted or assisted in forensic computer examinations for over ninety cases. Participated in over sixty searches.

PROFESSIONAL TRAINING

Sep 2015	*CART Basic Mobile Devices*, Linthicum, MD.
Jul 2015	*Sumuri MAC Forensics*, Dallas, TX. (5 days)

Jun 2015	*CART Unix Forensics,* Kansas City, KS. (5 days)
Jun 2015	*CART Virtualization Workshop*, Albuquerque, NM. (5 days)
Jan 2015	*SANS 518; MAC Forensics*, Seattle, WA. (6 days)
Jan 2014	*SANS Management 414; Training for CISSP*, Seattle, WA .(6 days)
Apr 2013	*CART Moot Court*, Norman, OK. (3 days)
Nov 2012	*CART Linux Command Line.* Albuquerque, NM. (3 days)
Aug 2012	*CART Practicals*, Stafford, VA. (5 days)
Jun 2012	*CART Intermediate; Web Artifacts.* Linthicum, MD. (3 days)
Jun 2012	*SANS 408*, Salt Lake City, UT. (6 days)
May 2012	*CART Intermediate; Operating System Artifacts.* Newark, NJ. (3 days)
May 2012	*CART Basic Tools*, Linthicum, MD. (3 days)
Mar 2012	*Digital Extraction Technician Class*. Stafford, VA. (9 days)

CERTIFICATIONS & AWARDS

Sep 2015	CART Macintosh Certification
Sep 2015	CART Unix Certification
Sep 2015	CART Cell Phone Certification
Sep 2014	Network + Certification - CompTIA
May 2014	GIAC Information Security Professional
Feb 2014	CART Mac Basic Certification
Dec 2012	CART Wintel Certification
Nov 2012	CART Linux Command Line
Aug 2012	GIAC Certified Forensic Examiner
Jun 2012	AccessData Certified Examiner
April 2012	CART Technician
Dec 2010	A+ Certification - CompTIA.