JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	No. CR15-5351RJB DECLARATION OF ROBERT YOUNG

I, Robert Young, declare under penalty of perjury that:

1. My name is Robert D. Young. I am the President of the Ability Systems, an Oregon Corporation specializing in the forensic analysis of computers and computer-based evidence. I have performed forensic software analysis and the analysis of computer storage media and communications networks since 1988. I have been accepted as an expert on computer forensic matters and have testified in numerous Federal, State and Municipal courts, including cases in the Federal District Court for the Western District of Washington. A list of cases and the venues I have testified in is provided in my curriculum vita, attached to this declaration.

2. Prior to drafting this declaration, I reviewed Mr. Michaud's Third Motion to Compel Discovery, the memos filed by the Government in response to that motion, and the declarations of Vlad Tsyrklevitch and Special Agent Daniel Alfin.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

3. I was retained last fall by the Federal Defender's Office as a defense consultant. In particular, I was retained to analyze Mr. Michaud's data storage devices (computer, thumb drives, etc.) to help determine exactly what the FBI's NIT did when it infected those devices; whether it exposed the devices to additional intrusions or hacking by compromising security settings; and the accuracy and reliability of any data allegedly seized by the FBI.

4. The Government notes in its Motion for Reconsideration that I have not yet done a forensic analysis of Mr. Michaud's data storage devices. Govt. Motion for Reconsideration at 8. The reason for that would be apparent to someone familiar with how this type of forensic analysis works.

5. Specifically, programs that run on a computer function as "object code," which is machine-ready binary ("ones and zeroes") content that instructs the computer's central processing unit ("CPU") what to do. Object code is created by taking human-readable source code written by a programmer and processing it with a "compiler" – a program that interprets the source code to generate the resulting object code.

6. Reverse engineering a program or NIT from object code is a lengthy, error-prone process that at best may only approximate the human-readable instructions written by the original programmer.

7. In addition, the NIT source code may include instructions that mask or conceal the object code, making it impossible to reverse engineer the code at all. Such code-hiding instructions typically include encryption (where a unique value is provided when the program is run to decrypt the instructions); non-sequential instruction flow (where the next action to be performed is not the next instruction in physical sequence); and dynamic code generation (where the set of instructions to be performed are created "on the fly" in temporary memory as the program runs and lost as soon as the program ends).

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

8. Moreover, when a program is delivered to a computer "dynamically" (such as with the NIT, which was sent as "hidden code" to target computers across the Internet), it is typically stored in volatile memory called "RAM." RAM data is lost as soon as power to the computer is removed. In other cases, the code may be stored in temporary disk storage, which is subject to frequent deletion and re-use.

9. Further, when a program like the NIT involves the use of a network, the instructions run on a single target computer may not provide enough information to determine what the program is doing. This is because the program on one computer can send information to another computer for processing by a completely different program, then rely on the results of this separate processing to determine what actions to take. As a result, the only way to understand the operation of a networked program on one computer is to inspect the relevant source code for all computers involved in the process. This is in part why, as explained in the declaration of Vlad Tsyrklevitch, an NIT consists of multiple "components." All of those components must be analyzed to determine how the NIT functioned and the reliability of the data collected by it.

10. Merely examining the output of the NIT or a "data stream" does not provide enough information about the program to determine if producing that output is all that the NIT does. Likewise, examining the forensic image of a computer that has previously run the NIT does not provide enough information to determine what the program may have changed, since the state of the computer before the NIT ran was not equally preserved. Moreover, while any data storage devices that were connected to Mr. Michaud's computer (like a disc or thumb drive) at the relevant times could be just as vulnerable or compromised as the computer itself, it is not possible to "reverse engineer" the NIT from those devices.

11. Another key consideration is the reliability of the "identifier" used on connection with seized data. While the Government insists the identifiers they generate

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

are unique (*see* March 28, 2016, Alfin Declaration at ¶¶ 8-10), I have learned over many years that, when it comes to computer forensics, simply saying something is unique or reliable does not make it true. Just like fingerprints analysis was considered uniquely reliable until it no longer was, in this case Vlad Tsyrklevitch has correctly stated in his declaration that there can be significant errors with how law enforcement agents generate identifiers.

13. In his declaration on this issue, Agent Alfin offers his personal assurances that the Government's evidence is reliable, but his declaration does not include, for example, such basic information as whether the FBI used a "unique number generator" program to create their ID numbers. If so, what algorithm and what "probability of collision" (chance of a duplicate) does that algorithm have? Did they just start at 1 and add 1 until they had a number that hadn't already been used? Does the identifier have an internal "checksum" to ensure there are no errors in transmission? Of course, any answers to these preliminary questions would still need to be verified by the defense, but the fact that the Government has not provided even basic information about how its identifiers are created and used is problematic in itself.

14. As a specialist in software and data forensic analysis, I have extensive experience with identifying malware and viruses, and I am also familiar with the many types of problems and issues that can arise when computer data is exposed to malware (such as an NIT). Without being allowed to review the discovery related to the operation of the NIT that the Court has already ordered, defense counsel would not be aware of all of the ramifications of the operation of the NIT on Mr. Michaud's computer and therefore may not be able to provide effective counsel to Mr. Michaud.

15. Finally, as someone who has participated in numerous secure, "closed room" code reviews, I am confident that the discovery ordered by the Court can be reviewed securely. It is my understanding that the Court has already entered a

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

protective order for the discovery and that the Government has not requested any changes to that order. In any event, Mr. Fieman has also informed me that the code analysis will be done by just one defense expert (Mr. Tsyrklevitch, who specializes in such analysis and has had security clearances), and that the defense has offered to have him review the discovery at a secure government facility. The FBI recently considered comparable arrangements adequate to ensure security for Apple's code during the recent litigation related to the San Bernardino, California shootings. Public disclosure of the Apple security bypass code (if the FBI had pursued the court order it obtained requiring Apple to create that code) would have had immediate and severe harms by exposing tens of millions of iPhone users (including law enforcement agents and government employees, journalists and activists in foreign countries) to hackers.

DONE this 2nd day of May, 2016.

Robert Young

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Curriculum Vitae, Qualifications, Testimony

Robert D. Young

Ability Systems Corporation
PO Box 6593
Aloha OR 97007
Tel: (503) 259-2614
FAX: (503) 802-9711
Robert@AbilitySys.com

Qualifications

Education and Experience

Robert D. Young received a Bachelors degree in Computer Science (BSCS) from Portland State University in 1984. He received a Masters degree in Business Administration (MBA) with Honors from Portland State University in 1991.

Mr. Young has over 36 years' experience in the computer industry and has held positions as varied as computer operator, applications programmer, systems analyst, systems programmer, technical support specialist and network manager. He has worked with a wide range of computers including mainframe computer systems, mini-computer systems and microcomputers (PCs) and programmable device (such as "smart' phones), along with the networks that connect them. Among his accomplishments are the designing and implementing of secure network connections between government agencies in the Portland, Oregon area, the design and installation of both PC networks and mainframe systems for the nationwide cold-storage firm Americold, and the design, implementation and management of a company wide auditor-support computer network for US Bancorp.

In 1986, Mr. Young helped start the Portland Area Network Users Group, a forum for users of PC networking software. He also assisted in the formation of the international Novell user organization. His responsibility included serving on the board of the Portland user group chapter representing them at international meetings, and has been awarded a lifetime membership in recognition of his efforts.

Since 1988, Mr. Young has received formal training in software and computer forensics, including the validity and infringement analysis of patents, trade secret evaluation and source code copyright analysis under the auspices of Johnson-Laird, Inc... For the past 24 years he has worked as a forensic software analyst, specializing in the preservation, production and analysis of computer-based evidence. Since 1990, Mr. Young has been the president of the Ability Systems Corporation, an Oregon corporation that provides computer forensic services.

Mr. Young specialties include software methodology and claim analysis for patent infringement, Cyber-Forensics® (performing plagiarism assessment of computer software for purposes of assessing copyright infringement) and performing authorship analysis for misappropriation of trade secrets. Mr. Young has extensive experience in the administration and analysis of software "clean room" environments, including work for a large software company developing competitive products. Mr. Young also specializes in Techno-Archeology®, the analysis of failed software development projects (projects that fail to meet contractual requirements or that are terminated for cause prior to completion), multimedia and digital video analysis, and computer-based evidence preservation, recovery, and analysis.

Publications And Papers Presented

Publications

"Login Scripts" PortLAN Newsletter (ISSN 1044-0739), February, 1993

"BrainShare '93" PortLAN Newsletter, May, 1993

"Btrieve Tales of Woe" PortLAN Newsletter, October, 1993

Papers Presented

"Forensic Computer Analysis and what it means to Network Administrators," Bellingham Computer Management Group, Bellingham, Washington, October 1998

"Maintaining the confidentiality of your computer-based records," Bullard, Korshoj, Smith & Jernstedt client briefing, Portland, Oregon, October 1999

"*Computer Based Evidence, or 'What's so bad about paper?'*" Lane, Powell, Spears & Lubersky, Portland, Oregon, November 1999 (CLE).

"Information Technology Basics," The Computer Law Association Cyberspace Camp, San Jose, California, March 2000.

"The camera (and computer) cannot lie. But they can be an accessory to untruth," Oregon Criminal Defense Lawyers Association Annual Conference, Bend, Oregon, June 2000.

"Data Security: Practical Tips For Effective Security And Privacy Policies," Law Seminars International Doing Business On Line Conference, Seattle, Washington, October 2000

"Three Phases of Forensic Evidence Analysis," 2001 Federal Public Defenders Computer Systems Administrator Conference, San Diego, California, June 2001

"Computer Forensics: What You Should Know About What the Cops Know," Oregon Criminal Defense Lawyers Association Seminar, Portland, Oregon, February 2004

"Computer Evidence Analysis: How evidence is found and what it can mean," Boston Federal Public Defenders, Boston, Massachusetts, March, 2006

"Computer Forensics for Defense Counsel," CJA Panel Attorney Training, Baltimore, Maryland, May, 2006

"Computer Evidence," Federal Public Defenders of Utah, Salt Lake City, Utah. January 2012

Expert Testimony

Since 1988, Mr. Young has performed patent, trade secret and copyright analysis as well as computer forensic analysis on several matters that did not (or have not yet) required testimony. These include preliminary work in anticipation of filing a lawsuit, and analysis work done to ensure a company is prepared to defend itself against an anticipated lawsuit. The following cases are matters for which Mr. Young's work has been disclosed:

Trial Testimony

1. Circuit Court of Oregon, Multnomah County, *State of Oregon vs. Barney Jean*, Case 99-06-34279, September 1999

2. Circuit Court of Oregon, Multnomah County, *State of Oregon vs. Christopher Hopkins Ediger*, Case 00-03-32855, October 2000

3. Testified regarding computer evidence before Grand Jury of Philadelphia, November 2000

4. Superior Court of California, San Diego County, *Information Management Group International, Inc. vs. Telecom Solutions et al.*, Case 721937, December 2000

5. United States District Court for the State of Utah, Central Division, *United States of America vs. Jeffery Tucker*, 98 CR 425C, January 2001

6. Court of Common Pleas of Philadelphia County, Pennsylvania, Family Court Division, Domestics Relations Branch, *Stuart A. Neill vs. Heather A. Dials Neill*, D.R. No OC0100078, May/June 2001

7. United States District Court for the Southern District of Florida, *United States of America vs. Herbert Pierre-Louis*, 00-434-CR-GOLD, September 2001

8. United States District Court, Western District of Missouri, Western Division, *Pioneer Financial Services, Inc. vs. Omni Financial Corporation*, No. 99-1212-CV-W-2, September 2001

9. United States District Court, Northern District of California, *Asian Communications Pty Ltd., et al., vs. Zi Corporation*, Case C-00-0989 PJH, August 2002

10. Circuit Court of Oregon, Multnomah County, *State of Oregon vs. Harry Robert Ketchum III*, Case 02-02-31097, October 2002

11. United States District Court, Southern District of Alabama, *United States of America vs. Avrahom Yeshurom Kaiser*, Case MJ02-0097-M, November 2002

12. District Court of Tarrant County, Texas, 67th Judicial District, *American Airlines, Inc. vs. FareChase, Inc.*, Case 067-194022-02, February 2003

13. District Court of Dakota County, Minnesota, *State of Minnesota vs. Brian Victor Myrland*, Case C8-01-2223, April 2003

14. United States District Court, District of Oregon, *United States of America vs. Robert Ian Greathouse*, Case CR02-476-KI, September 2003

15. District Court of El Paso County, Colorado, *State of Colorado vs. Sanford B. Schupper*, Cases 96CR1193, 01CR2859 and 01CR2889, September 2003

16. United States District Court, District of Oregon, *United States of America vs. James M. McLennan*, Case CR02-477-HA, October 2003

17. United States District Court, District of Utah, *United States of America vs. David Benjamin Mosier aka Scott Calvin*, Case 1:03CR00145TS, March 2004

18. District Court of El Paso County, Colorado, *State of Colorado vs. Jodi LeBlanc*, Case 202CR4437, March 2004

19. United States District Court, Western District of Washington at Tacoma, *United States of America vs. Robert Charles Lee*, Case 03-5120M, September 2004

20. United States District Court, Central District of California, *United Autocomp Computer, Inc. vs. Global Credit Services, Inc.*, Case SA CV 02-413 DOC (ANx), October 2004 (Neutral)

21. United States District Court, Western District of Pennsylvania, *Viad Corp. vs. C. Alan Cordial, Clifford E. Hellberg and Calan Communications*, Civil Action No. 03-1408, October 2004

22. Circuit Court of Oregon, Multnomah County, *Lisa Benitez vs. Neil Mages*, Case 04-09-69955, December 2004

23. Circuit Court of Oregon, Clatsop County, *State of Oregon vs. Andrew William Betnar*, Case 03-1274, January 2005

24. District Court of Salt Lake County, Utah, *State of Utah vs. Justin Blaine Davila*, Case 031902950FS, March 2005

25. United States District Court, District of Oregon, *United States of America vs. James M. McLennan*, Case CR02-477-HA, April 2005

26. Circuit Court of Oregon, Clackamas County, *State of Oregon vs. Gregg Bryant Ritchie*, Case 04-11509, June 2005

27. United States District Court, District of Oregon, *United States of America vs. Andrew ilcauskas and Robert Bloodgood*, Case CR04-423-HA, January 2006

28. United States District Court, District of Oregon, *United States of America vs. Timothy Olander*, Case CR06-75-HA, September 2006

29. United States District Court, District of Oregon, *United States of America vs. William Brook Knowles*, Case CR07-742JKB, August 2007

30. Superior Court of New Hampshire, Belknap County, *New Hampshire Ball Bearings, Inc., vs W. Scott Jackson, Sargent Controls And Aerospace, and Does 1-10*, Case 06-E-0106, November 2007

31. Circuit Court of Oregon, Lane County, *State of Oregon vs. Barry Barger*, Case 20-08-01740, February 2008

32. United States District Court, Western District of Texas, El Paso Division, *United States of America vs. Arkon Christopher Caldwell*, Case EP:07-CR-01512, March 2008

33. United States District Court, Western District of Washington, *United States of America vs. Kenneth Gouin*, Case CR 05-433 RSL, March 2008

34. Circuit Court of Oregon, Lane County, *State of Oregon vs. Barry Barger*, Case 20-08-01740, March 2008

35. Circuit Court of Oregon, Josephine County, *State of Oregon vs. Carvel Gordon Dillard*, Case 06-CR-0615, May 2008

36. United States District Court, District of Oregon, *United States of America vs. Charles E. Tarbell*, Case CR08-23-KI, June 2009

37. United States District Court, Western District of Washington, *United States of America vs. Joshua Osmun Kennedy*,, Case CR08-354RAJ, August 2009

38. Montana Fourth Judicial District Court, Missoula County, *State of Montana vs. Alexander Hovey*, Case DC-08-456, November 2009

39. United States District Court, District of Oregon, *United States of America vs. John Henry Ahrndt*, Case 08-CR-468-KI, January 2010

40. United States District Court, District of Oregon, *United States of America vs. Terrance S. Carpenter*, Case 08-000049-001, February 2010

41. United States District Court for the Western District of Texas, Austin Division, *Myriad Development, Inc. vs. Alltech, Inc.*, Case No. A-08-CV-253-55, March 2010

42. Circuit Court of Oregon, County of Klamath, *Matter of Taarna Finly, Korben Finley and River Finley*, Case 0900299JV1-3, November 2010

43. Superior Court of Washington, County of Clark, *State of Washington vs. Trevor Thomas Hutchinson-Flaming*, Case 10-1-00-918-3, February 2011

44. Utah Sixth Judicial District Court, Sevier County, *State of Utah vs. Donald Mitchell*, Case No. 071600174FS, April, 2011

45. General Court Martial, United States Army, Fourth Judicial Circuit, Joint Base Lewis McChord, *United States v. PFC Ronald Washington*, June 2011

46. Superior Court of California, Santa Cruz County, *State of California v. Richard Nelson Nash*, Case FI8291, October 2011

47. United States District Court For The Western District Of North Carolina, Charlotte Division, *Bridgetree, Inc. and Two Bit Dog, LLC vs. Red F Marketing LLC, Target Point, LLC, Daniel Roselli, Teng Li, Jason Li, Mali Xu, Mark Epperly and Elton T. Scripter*, Case Number 3:10-CV-228, February 2012

48. Circuit Court of Oregon, County of Marion, *Mark Long v. John Kroger in his official capacity as Attorney General for the State of Oregon*, Case 11C14422, March 2012

49. Superior Court of California, Santa Cruz County, *State of California v. James Edward Taylor*, Case (unknown), May 2012

50. United States District Court for the Eastern District of North Carolina, Western Division, *Silicon Knights, Inc. vs. Epic Games, Inc.*, Civil Action No. 5-07-CV-00275-D, May 2012

51. United States District Court For The Western District Of North Carolina, Charlotte Division, *Bridgetree, Inc. and Two Bit Dog, LLC vs. Red F Marketing LLC, Target Point, LLC, Daniel Roselli, Teng Li, Jason Li, Mali Xu, Mark Epperly and Elton T. Scripter*, Case Number 3:10-CV-228, August 2012

52. United States District Court for the State of Utah, Central Division, *United States of America vs. Michael L. Dunn*, 2:09-cr-00895-DB-1, October 2012

53. United States District Court, District of Oregon, *United States of America vs. John Henry Ahrndt*, Case 08-CR-468-KI, November 2012

54. United States District Court for the State of Utah, Central Division, *United States of America vs. Michael L. Dunn*, 2:09-cr-00895-DB-1, January 2013

Deposition Testimony

1. District Court of Travis County, Texas, 200th Judicial District, *BMC Software, Inc. vs. Peregrine Systems, Inc et al.*, Case 95-10161

2. Circuit Court of Oregon, Multnomah County, *Allstate Insurance Company vs. First Healthcare et al.*, Case 9907-07260

3. United States District Court for the Southern District of California, *WebSideStory, Inc. vs. WebTrends Corporation*, Case 99CV2498 BTM (RBB)

4. Superior Court of California, San Diego County, *Information Management Group International, Inc. vs. Telecom Solutions et al.*, Case 721937

5. United States District Court for the Eastern District of Virginia (Alexandria Division), *Dr. Bradley S. Fordham vs. OneSoft Corporation et al.*, Case 00-1078-A

6. United States District Court, Western District of Missouri, Western Division, *Pioneer Financial Services, Inc. vs. Omni Financial Corporation*, No. 99-1212-CV-W-2

7. United States District Court, Northern District of California, *Asian Communications Pty Ltd., et al., vs. Zi Corporation*, Case C-00-0989 PJH

8. United States District Court, District of Connecticut, *Narain C. Scott, et als. vs. Aetna Services, Inc.*, Case 3:01 CV 0046 (CFD)

9. District Court of Travis County, Texas, 126th Judicial District, *Recruitsoft, Inc. and Recruitsoft (Canada) Corporation, Inc. v. Claude Girard and Hire.com, Inc.*, Case GN-301147, August 2003

10. United States District Court, Southern District of New York, *Lamda Data Systems and P&C Insurance Systems, Inc. vs. Policy Administration Solutions, Inc. and Peter Pantelides*, Case No. 02 CV 8693 (RCC)(THK), October 2003

11. United States District Court, District of Massachusetts, *Knowledge Mechanics, Inc. vs. Outstart, Inc., John Alonzo and Michelle Bruce*, Civil Action 01-11178-GAO, November 2003

12. United States District Court, District of Arizona, Phoenix Division, *Lexcel Solutions, Inc. vs. MasterCard International Incorporated and MasterCard International, LLC*, Civil Action No. CV 03-1454PHX-JAT, August 2004

13. United States District Court, Western District of Pennsylvania, *Viad Corp. vs. C. Alan Cordial, Clifford E. Hellberg and Calan Communications*, Civil Action No. 03-1408, October 2004

14. United States District Court, Western District of Pennsylvania, *Medrad, Inc. vs. Tyco Healthcare Group LP, Mallinckrodt Inc., Liebel-Flarsheim Co. and Nemoto Kyorindo Co., Ltd.*, Civil Action No. 01-1997, June 2005

15. United States District Court, District of Delaware, *Affinion Loyalty Group, Inc. v. Maritz, Inc.*, Civil Action No. 04-360-JJF, June 2006

16. United States District Court, Southern District of Ohio, Western Division, *Market Scan Information Systems, In. vs. The Reynolds and Reynolds Company, Inc. et al.*, Case No. 3-06-CV-0254, November 2006

17. Superior Court of New Hampshire, Belknap County, *New Hampshire Ball Bearings, Inc., vs W. Scott Jackson, Sargent Controls And Aerospace, and Does 1-10*, Case 06-E-0106, January 2007

18. United States District Court, Southern District of Ohio, Western Division, *Market Scan Information Systems, In. vs. The Reynolds and Reynolds Company, Inc. et al.*, Case No. 3-06-CV-0254, February 2007

19. Superior Court of New Hampshire, Belknap County, *New Hampshire Ball Bearings, Inc., vs W. Scott Jackson, Sargent Controls And Aerospace, and Does 1-10*, Case 06-E-0106, October 2007

20. United States District Court, District of Oregon, *Alternative Legal Solutions. Inc. dba Compli vs. Ferman Management Services Corp., Mosaic Interactive LLC and Stephen B Straske II*, Case No. CV07-880-ST, November 2008

21. United States District Court for the Western District of Texas, Austin Division, *Myriad Development, Inc. vs. Alltech, Inc.*, Case No. A-08-CV-253-55, July 2009

22. United States District Court for the Northern District of Texas, Dallas Division, *Gillani Consulting, Inc. vs. Ferguson Enterprises, Inc..*, Civil Action No. 3-07CV1488-0, March 2010

23. United States District Court for the Eastern District of North Carolina, Western Division, *Silicon Knights, Inc. vs. Epic Games, Inc.*, Civil Action No. 5-07-CV-00275-D, May 2010

24. Superior Court Of The State Of California, County Of Santa Clara, *Monolithic Power Systems, Inc. vs. Wei Chen*, Case No.110-cv-172961, November 2011

25. United States District Court For The Western District Of North Carolina, Charlotte Division, *Bridgetree, Inc. and Two Bit Dog, LLC vs. Red F Marketing LLC, Target Point, LLC, Daniel Roselli, Teng Li, Jason Li, Mali Xu, Mark Epperly and Elton T. Scripter*, Case Number 3:10-CV-228, January 2012