UNITED STATES DISTRICT COURT
FOR DISTRICT OF MASSACHUSETTS

DAVID HOUSE,

Plaintiff,

v.

JANET NAPOLITANO, in her official capacity as Secretary of the U.S. Department of Homeland Security; ALAN BERSIN, in his official capacity as Commissioner, U.S. Customs and Border Protection; JOHN T. MORTON, in his official capacity as Assistant Secretary of Homeland Security for U.S. Immigration and Customs Enforcement,

Defendants.

Case No.
1:11-cv-10852-DJC

PLAINTIFF'S STATEMENT OF MATERIAL FACTS AND RESPONSE TO DEFENDANTS' STATEMENT OF MATERIAL FACTS PURSUANT TO LOCAL RULE 56.1

Pursuant to Local Rule 56.1, Plaintiff David House submits herewith a concise statement of the material facts as to which there are genuine issues to be tried and responds to Defendants' Concise Statement of Material Facts.

Plaintiff's Statement of Material Facts

1. Plaintiff was detained at O'Hare because his involvement with the Bradley Manning Support Network was being investigated by agencies other than Immigration and Customs Enforcement ("ICE") and Customs and Border Patrol ("CBP"). Months before this incident, Plaintiff had been placed on the government's TECS II watch list by an undisclosed government agency which resulted in the tracking of his international travel.

Declaration of David House, dated September 19, 2011, at ¶ 5 (hereinafter "House Decl.") (Attached as Ex. 1). Federal agents were waiting for Plaintiff when his plane landed at O'Hare airport in order to alert ICE and CBP to be prepared to detain and search his electronic devices. *See id.* ¶¶ 4-7, 10. Only after he had been admitted to the United States, after his belongings had been searched in the course of a secondary inspection, and after he was told that he was free to go was Plaintiff detained by Special Agents Louck and Santiago. *Id.* ¶¶ 5-6. Knowing exactly who he was, the two agents immediately confiscated Mr. House's netbook computer, USB storage device, digital camera, and cell phone. *Id*. ¶ 6. Mr. House was then taken to a separate room for interrogation, where he was questioned about his affiliation with the Bradley Manning Support Network and why he visited Manning in prison. *Id.* ¶ 8. Mr. House and his companion were detained for over an hour before they were permitted to leave. *Id.* ¶ 11.

2. The detention and seizure of Mr. House's electronic devices, along with the retention and sharing of the information stored on them, were not incident to a lawful border search. In support of their threshold motion for summary judgment, Defendants have submitted the sworn statements of Special Agents Louck and Santiago. These statements describe the general responsibilities of ICE and the fact that the agents were assigned to the Chicago ICE office, but neither statement explains the responsibilities of the two agents on November 3, 2010, nor their purpose in detaining Mr. House and seizing his electronic devices. *See* Declaration of Marcel Santiago, dated July 27, 2011, Defs.' Concise Statement of Material Facts Pursuant to Local Rule 56.1 (hereinafter "Defs.' Facts"), Ex. 2; Declaration of Darin Louck, dated July 27, 2011, Defs.' Facts, Ex. 3.

3. The substantial delay in returning Mr. House's computer and other devices was not solely attributable to the password protection of his computer, its dual boot configuration, the technical requirements of verifying the imaging of the computer, and the workload of ICE computer forensics technicians, as Agent Marten claims. Declaration of Robert Marten, dated July 27, 2011, at ¶¶ 10-13, Defs.' Facts, Ex. 4 (hereinafter "Marten Decl."). Forensic imaging of a computer's hard drive using standard software can be completed in a matter of a few days, if not sooner. Declaration of Alexander Stamos, dated September 20, 2011, at ¶ 6 (hereinafter "Stamos Decl.") (Attached as Ex. 2). The process is not delayed by the absence of a password as imaging produces a copy that is not password protected. Stamos Decl. ¶ 20. The devices were detained for a period of one week before being received in New York and were not received by Mr. House until December 22, 2010. *See* Marten Decl. ¶¶ 5, 7; House Decl. ¶ 14.
4. Defendants have conceded for purposes of this stage of the litigation that copies of Mr. House's information were shared with other agencies and are being retained by those agencies. Compl. ¶ 27.[1] ICE Directive 7-6.1, § 8.5 provides for the sharing and retention of information by other federal agencies for various reasons. Defs.' Facts, Ex. 5. Defendants have submitted the sworn statement of Special Agent Marten in support of their threshold motion for summary judgment, which discusses only the copies retained by ICE itself. Marten Decl. ¶ 15. The declaration is silent about whether other copies were made, shared, and still exist. For purposes of Defendants' motion to dismiss, therefore, Defendants have conceded the allegation in Plaintiff's complaint that

[1] Although it is normally inappropriate to rely in a statement of material facts on allegations found in a complaint, Plaintiff does so here only to the extent that allegations contained in the complaint have not been put into dispute by Defendants' declarations.

information copied from his computer has been shared with and retained by other government agencies.

5. Copies of information from Mr. House's devices were not retained merely for purposes of this litigation. At the time the devices were returned, ICE was unaware that Mr. House was represented by counsel or that litigation was contemplated. When counsel for Mr. House wrote to the Defendants on December 21, 2010, there was no mention of litigation. Declaration of John Reinstein, dated September 20, 2011, at ¶ 3c, Pl.'s Opp'n to Defs.' Mot. to Dismiss, or in the Alternative, for Summ. J., Ex. 1 (hereinafter "Reinstein Decl."). This action, which seeks destruction or return of the information, was not filed until May 2011, six months after the seizure of Mr. House's devices and four and one half months after their return. The only active litigation at the time the copies were made was the prosecution of Pfc. Bradley Manning. Reinstein Decl. ¶ 3(c).

<u>Response to Defendants' Statement of Undisputed Facts</u>

1. Admitted.
2. Plaintiff disputes the notion that he was simply "referred" for secondary screening and then questioned.
3. Admitted.
4. Plaintiff admits that the ICE agents returned his cell phone and detained the remaining items, but asserts that no reason was provided for their detention and that these items were seized and detained without reasonable suspicion. Compl. ¶ 31.
5. Plaintiff admits that he was stopped as he was leaving the area where his belongings were searched and that he was taken to a government office where he was detained

for over one hour. House Decl. ¶¶ 7, 11. Plaintiff cannot admit or deny that he was in the "Federal Inspection Service Area" when he spoke with government agents. In any event, this term has no legal significance.

6. Denied. After the search of his belongings in the course of secondary screening, Plaintiff was told that he was free to leave. House Decl. ¶¶ 5-6.

7. Denied. Plaintiff's devices were seized by ICE on November 3, 2010. They were not returned to him until December 22, 2010, seven weeks after they were seized. House Decl. ¶ 14. The devices were sent to an ICE facility in New York approximately one week after their seizure. Marten Decl. ¶ 5.

8. Denied. The devices were sent to Plaintiff via FedEx on December 21, 2010, and were received on December 22, 2010. House Decl. ¶ 14.

9. Plaintiff admits that while his devices were detained by ICE, images of the detained media were forensically prepared and reviewed. The qualifications of the individual responsible for imaging and review are neither described nor established by the Marten Declaration.

10. Plaintiff admits that a purpose of forensic imaging is to ensure that the imaged data is intact and accessible for review.

11. Plaintiff admits that a purpose of forensic imaging is to ensure that the original evidence is not disturbed. Plaintiff disputes that the process of imaging caused the delay in returning his property. Stamos Decl. ¶ 6.

12. Plaintiff admits that he was asked for passwords to access his computer and stated that he explained he could not disclose a password because the computer contained proprietary material belonging to his employer. House Decl. ¶ 7. Plaintiff asked

Agents Louck and Santiago whether he was required by law to disclose his password but did not receive a response. House Decl. ¶ 7.

13. Plaintiff disputes that his failure to provide passwords justified the extended detention of his property. The processes of imaging and verification described in the Marten Declaration should not have taken more than 18 hours. Stamos Decl. ¶ 6. The process is not delayed by the absence of a password, which is "completely irrelevant" to any of the standard imaging methods. Stamos Decl. ¶ 20.

14. Plaintiff admits that his laptop contained both a Windows and a Linux operating system. The partition of a computer's hard drive and the use of a dual boot system employing different operating systems on a single computer is not "non-standard" and is not unusual. Stamos Decl. ¶ 21. The Linux operating system is widely used. Stamos Decl. ¶ 21. Neither the use of a dual operating systems nor the use of Linux would delay the process of imaging. Stamos Decl. ¶ 21.

15. Plaintiff admits that most personal computers use Windows and Macintosh based operating systems. At present, Plaintiff lacks sufficient information to respond to the statement concerning the practice of ICE forensics agents. A properly trained and certified computer forensic technician would be familiar with the Linux operating system and with dual boot systems. Stamos Decl. ¶ 21.

16. Denied. This process did not have to occur. The verification step should have been performed during the initial capture of the hard drive and does not require any additional software. Stamos Decl. ¶ 22. Some groups consider it best practice to build a new forensics workstation for each project, but this step can be automated to occur very quickly and, at worst, should take only about four hours to install the

requisite new operating system and forensics software package. *Id.* At present, Plaintiff lacks sufficient information to respond to the statement concerning the imaging of his computer by ICE technicians.

17. At present, Plaintiff lacks sufficient information to respond to this statement.
18. At present, Plaintiff lacks sufficient information to respond to this statement.
19. At present, Plaintiff lacks sufficient information to respond to the statement concerning the procedures followed by ICE and whether those procedures were consistent with ICE Directive No. 7-6.1.
20. Plaintiff admits that ICE is retaining copies of his devices "only for purposes of litigation" but notes that Defendants have not indicated *which* litigation, whether this litigation or some other investigation or criminal proceeding. Moreover, ICE is not the only defendant in this case; Plaintiff also sues Customs and Border Protection and the Department of Homeland Security. Defendants have not offered a complete picture of all the agencies that copied, received, or retained the contents of Mr. House's electronic devices.

Respectfully submitted,

DAVID HOUSE
By his attorneys,
___/s/ *Catherine Crump*_____
Catherine Crump, Pro Hac Vice
ccrump@aclu.org
Speech, Privacy and Technology Project
American Civil Liberties Union
125 Broad Street, 17th floor
New York, New York 10004
(212) 549-2500

____/s/ *John Reinstein*_______
John Reinstein, BBO # 416120

jreinstein@aclum.org
Laura Rótolo, BBO # 665247
lrotolo@aclum.org
Alexia De Vincentis, BBO # 679397
adevincentis@aclum.org
American Civil Liberties Union
of Massachusetts
211 Congress Street
Boston, Massachusetts 02110
(617) 482-3170

September 21, 2011

CERTIFICATE OF SERVICE

I hereby certify that the foregoing document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non registered participants by First Class Mail, on the 21st of September, 2011.

*/s/ Catherine Crump*__
CATHERINE CRUMP
September 21, 2011

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

DAVID HOUSE,)
)
Plaintiff,)
)
)
)
JANET NAPOLITANO, in her official capacity as) Case No. 1:11-cv-10852-DJC
Secretary of the U.S. Department of Homeland)
Security; ALAN BERSIN, in his official capacity as)
Commissioner, U.S. Customs and Border Protection;)
JOHN T. MORTON, in his official capacity as Director,)
U.S. Immigration and Customs Enforcement,)
)
Defendants.)

INDEX TO ATTACHMENTS TO PLAINTIFF'S STATEMENT OF MATERIAL FACTS AND RESPONSE TO DEFENDANTS' STATEMENT OF MATERIAL FACTS PURSUANT TO LOCAL RULE 56.1

EXHIBIT #	DESCRIPTION
1	Declaration of David House, dated September 19, 2011
2	Declaration of Alexander Stamos, dated September 20, 2011

EXHIBIT 1

UNITED STATES DISTRICT COURT
FOR DISTRICT OF MASSACHUSETTS

DAVID HOUSE,

Plaintiff,

v.

JANET NAPOLITANO, in her official capacity as Secretary of the U.S. Department of Homeland Security; ALAN BERSIN, in his official capacity as Commissioner, U.S. Customs and Border Protection; JOHN T. MORTON, in his official capacity as Assistant Secretary of Homeland Security for U.S. Immigration and Customs Enforcement,

Defendants.

Case No.
1:11-cv-108520-DJC

DECLARATION OF DAVID HOUSE

I, DAVID HOUSE, hereby declare the following:

1. In May 2010, Bradley Manning, a U.S. serviceman deployed in Iraq, was arrested on suspicion of having disclosed restricted material to the organization WikiLeaks. In July 2010, he was formally charged with accessing and disclosing without authorization classified information, including “a classified video of a military operation,” and fifty Department of State cables. Further charges were brought against him in March 2011, including a charge that he knowingly gave intelligence to the enemy, a capital offense.

2. In June 2010, I joined with other individuals to establish the Bradley Manning Support Network ("Support Network"). The Support Network takes the position that Manning is accused of being a whistle blower who brought to light misconduct by U.S. armed forces personnel and has undertaken to inform the public of the issues raised by Manning's prosecution, to coordinate international support for Manning, to raise funds for his legal defense, and to provide him with support during his imprisonment.

3. On November 3, 2010, following a vacation in Mexico, I arrived at Chicago O'Hare International Airport en route to Boston.

4. As the plane arrived at O'Hare, an announcement was made that everyone should have their passports out to be checked by government officials on the jetway as we deplaned. Leaving the plane, I observed two uniformed agents taking people's passports, checking them, and giving them back. When I handed the agents my passport, they checked it, looked at each other, and handed it back to me. The agents then turned around and left the jetway, neglecting to check the documentation of any of the passengers deplaning after me.

5. I proceeded to pass through a passport control station and was admitted for entry into the United States as a U.S. citizen. I was referred to secondary screening, where my belongings and those of my travel companion were searched by a Customs and Border Patrol ("CBP") agent and I was questioned about whether I had been using my computer. I have since learned that at some time prior to September 2010 my name was placed on the federal government's TECS II watch list, which tracks my international travel and results in additional screening on entering the United States.

6. Following the search of my belongings, I was told that I was free to go and walked towards the terminal to make my connecting flight to Boston. At that point, I was stopped by Special Agents Louck and Santiago of Immigrations and Customs Enforcement ("ICE"). The agents identified themselves and required, without any explanation, that I give them my laptop computer, USB storage device, digital camera, and cellular phone. The devices were taken to an undisclosed location.
7. I was taken to a separate, closed room for interrogation, where I was initially asked questions concerning the security of my computer. When the agents requested the password to log on to my computer, I explained that I could not disclose it because the computer contained proprietary material belonging to my employer. I asked the agents if I was required by law to disclose the password but did not receive a response.
8. I was next asked about my affiliation with the Bradley Manning Support Network, why I visited Bradley Manning in prison, what I thought about WikiLeaks, and whether I had been in contact with anyone from WikiLeaks while I was in Mexico. The agents also questioned my travel companion, asking similar questions about whether she was affiliated with the Support Network and what she thought about WikiLeaks.
9. Neither I nor my travel companion were asked any questions relating to border control, customs, trade, immigration, or terrorism, and at no point did the agents suggest that we had broken the law or that my computer contained any illegal material.

10. At the conclusion of this questioning, the ICE agents returned my cell phone but detained my laptop computer, USB device, and digital camera. I was given a receipt for the items and was told that they would be returned within a week.
11. After being detained for over an hour, we were permitted to leave.
12. The computer seized from me by the ICE agents was a netbook with a partitioned hard drive utilizing two operating systems, Linux and Windows.
13. The hard drive of my computer was password protected and contained proprietary information from the Massachusetts Institute of Technology, my employer at the time of the seizure.
14. I received my electronic devices on December 22, 2010, 49 days after they were seized. The devices were shipped to me via FedEx from the "DHS CIS New York District Office."
15. One day prior to receiving my devices, I sent a letter, though counsel, to the Department of Homeland Security ("DHS"), CBP, and ICE requesting that the devices be returned and requesting that I be provided with documentation of the chain of custody of any copies made of the information contained on the devices and documentation of their destruction.
16. In a letter dated December 30, 2010, general counsel for ICE noted that my devices had been returned but did not indicate whether the information contained on the devices was copied, to what agencies or individuals those copies were provided, and whether any such copies had been destroyed. The letter stated that the request for documentation would be treated as a request under the Freedom of Information Act.

17. As we did not receive a further response to the request for documentation, my attorneys made a separate Freedom of Information Act Request to ICE on February 4, 2011 requesting records concerning me and the seizure of my electronic devices. In response to that request, ICE refused to produce records concerning the chain of custody or sharing of information.

I declare under penalty of perjury that the foregoing is true to the best of my knowledge, information and belief.

David House

Date: 9/19/11

EXHIBIT 2

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

DAVID HOUSE,	)	
	)	
Plaintiff,	)	
	)	
v.	)	
	)	
JANET NAPOLITANO, in her official capacity as	)	Civil Action No. 11-10852-DJC
Secretary of the U.S. Department of Homeland	)	
Security; ALAN BERSIN, in his official capacity as	)	
Commissioner, U.S. Customs and Border Protection;	)	
JOHN T. MORTON, in his official capacity as Director,	)	
U.S. Immigration and Customs Enforcement,	)	
	)	
Defendants.	)	

DECLARATION OF ALEXANDER STAMOS

I, ALEXANDER STAMOS, hereby declare the following:

1. I have been retained by counsel for David House to analyze the government's justifications for the length of time it took to make verified forensic copies of Mr. House's electronic devices.

Background and Qualifications

2. I am a co-founder of iSEC Partners ("iSEC") and currently serve as its Vice President and the Chief Technical Officer. iSEC is an information security consulting firm headquartered in San Francisco, with offices in Seattle and New York and is a fully owned subsidiary of the NCC Group plc, headquartered in Manchester, UK. Our work includes software assurance, infrastructure penetration testing, code review, incident response and forensics. Our clients

include Microsoft, Oracle, eBay, McKesson, Salesforce.com, Google, Autodesk, Charles Schwab, JPMorgan Chase, Bank of America, Wells Fargo, ING Direct and Motorola.

3. Before founding iSEC Partners I worked as a Managing Security Consultant with the security consultancy @stake, and I was the security lead at Loudcloud, a managed hosting provider. I have also worked for the EO Lawrence Berkeley National Laboratory. I hold a BS in Electrical Engineering and Computer Science from the University of California, Berkeley, where my studies included graduate classes in networking and computer security. I was awarded a Certified Information Systems Security Professional (CISSP) certification in April 2003. I am a frequent speaker at leading security and technology conferences, such as Black Hat USA, CanSecWest, Microsoft BlueHat, the Web 2.0 Expo, CTIA, OWASP App Sec, and the FinancialServices Information Sharing and Analysis Center (FS-ISAC). I have also spoken on the topic of computer forensics to private audiences at the FBI's Regional Computer Forensics Laboratory, and the Federal Reserve Banks in New York and Boston.

4. Over the last six years I have been retained as an expert witness in seven separate civil litigation matters and performed as the technical lead for dozens of forensics and incident response projects. My forensics work includes investigations for Charles Schwab, Autodesk, Facebook and The Davidson Companies.

5. A copy of my resume is attached to this report.

Topic of Report

6. I have been asked to review the declaration of Robert Marten and to provide an opinion on whether the reasons set forth in paragraphs 10-12 of the declaration justify the extended period during which the devices were detained to make verified forensic copies. In my opinion, the process of imaging and verification described in the declaration should not have taken more

than 18 hours and did not require the one week period that the devices were retained by ICE in Chicago and certainly did not require the period of nearly six weeks that the devices were retained in New York.

Overview of the Process of Computer Forensics

7. Computer forensics is the use of scientific and technical means to determine what actions have been undertaken by users, software and remote attackers on a computing system. Computer forensics is mostly concerned with finding and analyzing the stored data on a computing system, also known as state. Examples of components that store state that can be examined during the forensics process include the system's hard disk drive, a solid state drive, external drives (such as Flash drives), optical media (such as burned compact discs) and the various types of system RAM.

8. Computer forensics is generally broken down into two broad categories, analysis of "live" and "dead" systems. Live systems are computers that are still running and therefore have retained state in the volatile Random Access Memory (RAM) of the system. RAM is used as scratch space for the operating system and running programs, and is generally not accessible to the end-user in the same way that the system's hard drives or external disks are via graphical interfaces like the Windows Explorer. Since it is very difficult to access the running system's RAM without causing changes to the evidence being gathered, the majority of forensics projects fall under the "dead" category, and live forensics is generally reserved for incident response investigations involving new malware or machines that are under active control by an attacker. Neither of those situations apply here, and since Marten does not give any indication that the system's RAM was imaged I will assume that ICE was performing dead system forensics per forensic best practice through the rest of this declaration.

9. The vast majority of forensically useful data from a laptop computer is contained on the laptop's hard drive, and although there are other types of state that can be collected by a forensic examiner there is no indication that anything other than the hard drive was of interest to Marten. I am using the term hard drive generically to include implementations that do not use a spinning metal disc, such as a solid-state drive (SSD). SSDs are functionally equivalent to traditional hard drives in almost all respects relevant to forensic examination.

10. As Marten explains in paragraph 7 of his declaration, it is generally considered best practice for a forensic examiner to make an identical bit-for-bit copy of a hard drive, verify that the copy is correct and to perform his investigation on the copy. The normal use of an operating system irrevocably changes the state of the hard drive in dozens of ways so forensic examiners generally never boot the target system during their investigation, instead they use one of four methods to image the hard drive in a way where they can prove that no changes to the hard drive occurred.

11. The first method is to remove the system's hard drive and connect it to a hardware write-blocker. These are specialized devices that interface with the target hard drive using the drive's native protocol (usually SATA) on one side and provide a more generic interface to the examiner's system on the other (such as USB or Firewire). The hardware write-blocker uses specialized logic to relay commands to read data from the drive but not commands to write data, and the use of these products is generally considered by forensic examiners as the easiest and safest way to capture a target drive. Equivalent technology also exists for safely reading USB flash drives as well as memory formats common to digitals cameras, such as compact flash (CF) and secure digital (SD). The speed of this technique is generally limited by the connection type used between the hardware write-blocker and the examiner's system.

12. The second method is to use software write-blocking. In this scenario, the examiner loads a specialized software product on his system that prevents the operating system from relaying write commands to the target device. This is generally considered an inferior solution, since software write-blockers are known to fail in ways that are difficult to detect and cannot block write commands issued by the underlying hardware. A popular commercial product that provides this kind of blocking is EnCase Forensic Edition.

13. The third method is the use of a high-speed forensics disk duplicator. This is a specialized piece of hardware that can operate without a connected computer system and which makes a verified copy of a hard drive onto another physical drive. This technique is often used for capture of hard drives in the field, since it can be much faster than other techniques and is generally only limited by the speed of the hard drive itself.

14. The fourth method is to boot an alternate operating system on the target system and to stream the system's hard drive across a network connection to the examiner's workstation. This is considered a more risky option, since a mistake by the examiner could lead to the target system booting into its standard operating system and modifying the disk. This technique is most useful when imaging data from computer servers with large or complicated disk arrays, which is not applicable to Mr. House's laptop.

15. All four of these techniques should be able to image a normal laptop hard drive in less than 12 hours, baring a serious hardware failure or rare types of hardware encryption. Marten mentioned neither a failure or hardware encryption mechanism in his declaration.

16. After a target disk is imaged using one of these methods it is then considered best practice to verify the accuracy of the copy by calculating a cryptographic hash of the drive and the copy. A cryptographic hash is a mathematical mechanism for generating a small fingerprint

from an arbitrarily large amount of data and can be used to detect any modification of forensic data during the examination process. Currently SHA1 is considered the best algorithm for calculating this fingerprint, although the older and less secure MD5 function is also often used for compatibility reasons. A proper cryptographic verification will read the target disk a second time to insure that no errors were inserted into the data stream during the copying process.

17. A wide variety of free and commercial software tools are available to perform the imaging, verification and examination of hard drives and external storage. Popular commercial products include Guidance Software's EnCase suite and AccessData Forensic Tool Kit (FTK). Popular free tools include dcfldd and The Sleuth Kit (TSK).

18. Forensic tools are able to access data that is not readily available during the normal operation of a computer system, including deleted, hidden and temporary files. This is another reason why it is important for a forensic examiner to make an exact copy of the target drive and to examine that copy on a separate workstation with special tools instead of booting the machine and viewing files via the operating system.

Creating Verified Forensic Copies of Mr. House's Electronic Devices

19. Marten ascribes the delay solely to problems in the making of two verified forensic copies of the data contained in Mr. House's computer. He identifies no factors explaining delay in the forensic examination of the flash drive and digital camera other than the issues of personnel and workload.

20. With regards to the lack of knowledge of a password, this should not affect the ability to make a verified forensic copy of the data or increase the amount of time necessary to do so. The standard forensic imaging process utilizes a method of copying the drive external to the system's normal operating system, and access to the user's password is completely irrelevant to any of the

four imaging methods I described previously. After the drive is imaged it is also not necessary to use a password to examine files on the disk, these files would be easily found and viewed by any of the tools I named previously. The only situation where a password is required to access data on a hard drive would be the use of disk or file encryption, and Marten makes no reference to those technologies being used by Mr. House.

21. With regards to having two operating systems, the partition of a computer's hard drive and the use of a dual boot system employing different operating systems on a single computer is not "non-standard" and is not unusual. For example, Apple provides a supported mechanism for dual booting modern Macintosh computers called Boot Camp, and dozens of tools to facilitate dual booting on PCs are available. The Linux operating system is widely used. A properly trained and certified computer forensic technician would be familiar with the Linux operating system and with dual boot systems. Having two operating systems does not increase the time required to copy the data. A forensic capture of a hard drive collects the entire drive and the speed at which this happens is independent of the contents of the drive. Forensically imaging a blank hard drive generally takes the same amount of time as one that is full of data. Likewise, all of the major free and commercial forensics products support examining hard drives with multiple operating systems, and all of them support the common Linux filesystem types. In a product such as EnCase or FTK, there would be no additional work necessary to capture and view the contents of a hard drive containing both Windows and Linux, although some examination steps after the initial imaging might need to be repeated for each OS.

22. In paragraph 12, Marten states that "Third, a separate computer had to be set up with forensic software to see if the images on Mr. House's devices had been made correctly. This set-up also took time and also required the time of an ICE computer forensics agent. ICE could only

return Mr. House's devices to him after the images had been verified on the reviewing computer as correct and accurate copies." In my opinion this should not have caused a delay, since the verification step should have been performed during the initial capture of the hard drive and does not require any additional software. Some groups consider it best practice to build a new forensics workstation for each project, but this step can be automated to occur very quickly and, at worst, should take about four hours of time to install a new operating system and a forensics software package.

[SIGNATURE /DATE]

Alex Sep 20, 2011

Alexander C. Stamos

213 Wellington Drive
San Carlos, CA 94070

Phone (415) 378–9580
E-mail alex@stamos.org

WORK EXPERIENCE

iSEC Partners, Inc. San Francisco, California
Founder and CTO October 2004 – Current

Co-Founder and CTO specializing in mobile application security, cloud computing infrastructures, secure system design and secure software engineering practices. During the early days of the company, was integral in the creation of the company's professional services organization and led internal operations. As the company grew, Alex headed a well-recognized research and evangelism effort while continuing to lead teams on some of iSEC's most challenging projects.

- Built a self-funded 5-person venture into a $24.2M exit to a public UK firm, NCC Group
- Concurrent responsibilities in finance, marketing, operations, and technical delivery
- Successfully managed and mentored 7 direct and 29 indirect reports, ranging from recent college graduates to experienced security experts
- Executed iSEC's media relations strategy through interviews, papers and high-profile speaking engagements
- Head of entire Professional Services organization. Successes include:
  - Defined iSEC's suite of services
  - Created project delivery and management model
  - Led professional services to excel in all customer satisfaction metrics, including an 80% return revenue rate and dozens of Fortune-500 clients
- Performed as technical lead on numerous consulting projects, including:
  - Design and security reviews of critical enterprise management systems
  - Was lead technical resource on numerous reviews of high profile web applications ranging from innovative startups to established Top-5 banks
  - Led several penetration tests and design reviews of a major commercial operating system
  - Managed the multi-company effort to design and test the Android security model for Google
  - Successfully reverse engineered a widely deployed DRM framework
  - Several critical cryptographic and system security reviews of high-availability financial systems
- Forensics, incident response and expert witness work includes:
  - Led investigation into foreign-government APT attacks against American businesses
  - Rapid incident response and system forensics on a high-profile financial industry intrusion, leading to successful international law-enforcement action
  - Investigation into a remote business intrusion leading to a quick settlement for the victim in a civil lawsuit
  - Workstation and smartphone forensics to investigate internal financial employee misconduct
  - Defensive investigation of patent claims leading to a successful outcome for the respondent
- Performed original application research and presented at leading conferences, becoming a recognized leader in web and mobile application security
- Created and delivered several acclaimed software security curricula to academic and corporate audiences
- Contributed chapters to *Hacking Exposed: Web 2.0* and *Mobile Application Security*

@stake, Inc. San Francisco, California

Senior Security Architect/Managing Security Architect September 2002 – September 2004

As a Managing Security Architect at @stake, Alex was responsible for every part of the consulting engagement lifecycle; from sales and project development to delivery and documentation. Performed as a technical lead or contributor on dozens of varied projects, ranging from low-level reverse engineering assignments to high-level network re-designs.

- Discovered several major vulnerabilities during a comprehensive penetration test and code review of a major web server platform
- Served as technical leader on a complex, six person, enterprise-wide network and host assessment
- Performed security assessments of 802.11 equipment using penetration testing and code review, once finding new cryptographic issues in a standards-track protocol
- Completed a solo re-architecture of a major software vendor's ASP network, resulting in greatly improved uptime, security, and manageability

Loudcloud, Inc. Sunnyvale, California

Security Engineer/Senior Security Engineer June 2001 – September 2002

At Loudcloud, was responsible for providing best-of-breed security solutions to Fortune 500, foreign government, and U.S. government customers. Was involved at every step of the security process: architecture, consultation, implementation, auditing, monitoring, incident response, and forensics. Alex also had personal responsibility for managing customer communication, sales support, patch levels, and for building Loudcloud's global security-monitoring infrastructure.

- Designed and implemented a new global Network IDS infrastructure, allowing Loudcloud to provide real-time intrusion detection and alerting across six global datacenters, with a minimum of day-to-day human interaction and maintenance
- Designed and engineered Loudcloud's Security Monitoring System, saving the company seven-figures in outsourcing costs
- From April 2002 on owned primary responsibility for customer and sales support for Loudcloud Security team
- Acted as lead responder to various security incidents, including DDoS attacks, worm infections, and penetrations of production servers

EDUCATION

University of California, Berkeley July 1997 – May 2001

B.S. in Electrical Engineering and Computer Science

- Chancellor, National Merit and Alumni Scholar
- Undergraduate research experience in clustered systems and software security
- Graduate courses in Computer Networking, Security and Cryptography
- Held undergraduate research positions in CS Department and at E.O. Lawrence Berkeley National Laboratory

SELECTED PRESENTATIONS AND PUBLICATIONS

"Vulnerabilities 2.0 in Web 2.0: Next Generation Web Apps from a Hacker's Perspective"
Presented at:

- Black Hat USA 2006
- Web 2.0 Expo 2007
- ACM Reflections/Projections Conference
- Black Hat Japan 2006
- ToorCon 8

"Rich Internet Applications: Blurring the Line Between Desktop and Web Security"
Presented at:

- Black Hat USA 2008
- Web 2.0 Expo Europe
- Defcon 16

"Mobile Web Security"
Presented at:

- California CISO Lecture Series
- ISSA Silicon Valley
- Web 2.0 Expo SF 2009

"Cloud Computing Security: Fuzzy Systems Provide Fuzzy Assurances"
Presented at:

- ISACA Los Angeles
- ISACA Orange County
- ISACA Silicon Valley Conference
- ISSA-LA Annual Meeting

"Cybercrime Today and Tomorrow's Threats"
Presented at:

- Web 2.0 Expo 2009
- O'Reilly Emerging Technology (ETech) Conference 2009

"Breaking Forensics Software: Weaknesses in Critical Evidence Collection"
Presented at:

- Black Hat USA 2007
- FBI Regional Computer Forensics Laboratory
- High Tech Crimes Investigation Association
- Defcon 15

"Code Scanning Tools: Success and Failure in the Field"
Presented at:

- ISACA Silicon Valley Annual Conference
- WOOT '08 Rump Session

"Cross Domain Request Forgery and Web Crimes"
Presented at:

- FBI Infraguard - SF Bay Winter Conference

"Attacking Web Services"
Presented at:

- CanSecWest/core06
- Black Hat USA 2005
- Software Security Summit
- InfoWorld SOA Executive Forum
- OWASP App Sec DC 2005