Declaration of Neil Broom

795 Hammond Drive Suite #1806 Atlanta GA 30328	Toll Free: 800-839-2088 Atlanta: 678-428-6304 Fax: 678-264-4900	Email: nbroom@trcglobal.com

Ceglia v. Zuckerberg and Facebook, Inc. No. 1:10-cv-569-RJA-LGF • June 4, 2012

DECLARATION OF NEIL BROOM - BACKGROUND AND EXPERIENCE

I am over 21 years of age and suffer from no disability and I am competent to make this affidavit. I do so from my own personal knowledge except where noted. I base my opinions on my knowledge, skill, experience, training, and education.

I am the Chief Executive Officer, Senior Investigator, and Laboratory Director for Technical Resource Center, Inc., (referred to as "TRC" in the remainder of this affidavit), a computer forensics and investigation practice firm headquartered in Atlanta, Georgia. I have personal knowledge of the matters described in the affidavit, knowledge which I acquired in the course of my duties for TRC.

I have over 16 years of experience providing investigative, technical, educational, and security services. I am a Certified Computer Examiner (CCE), a Certified Fraud Examiner (CFE), and a Certified Information Systems Security Professional (CISSP) and I co-authored a book in the field of Computer Forensics entitled Computer Forensics JumpStart. I have provided training in the fields of Computer Forensics and Information Security to over 3,000 students and I am a licensed Georgia Private Detective. I have presented testimony as an expert witness multiple times. A true and accurate copy of my Curriculum Vitae is provided herewith as Exhibit A.

TRC's laboratory has earned the prestigious ASCLD/LAB Accreditation in the field of Digital Evidence (Computer Forensics) from the American Society of Crime Laboratory Directors / Laboratory Accreditation Board. ASCLD/ LAB offers accreditation to forensic laboratories that exhibit strict compliance to a large number of rigorous quality standards. The accreditation program is voluntary and open to any laboratory. As of March 21, 2012 there are 57 laboratories currently accredited in the discipline of Digital & Multimedia Evidence including the FBI, the Regional Computer

Forensics Laboratories (RCFL), and the Drug Enforcement Administration (DEA).

I have performed and supervised computer forensic work on hundreds of computers, including laptops, workstations, personal digital assistants, and network servers.

To recover data, computer forensic specialists, such as myself, follow a standard methodology that is accepted in the field. That methodology involves documented and correct collection, imaging, analysis, and reporting methods. Collection methodology includes the use of documentation, write blockers, appropriate and approved forensic imaging hardware and software and verifying hash values, which are electronic fingerprints of the image. Analysis and reporting methodologies include documentation, production, keyword searches, running specialized forensic scripts and the use of appropriate and approved software tools such as Forensic Toolkit version 1.8.5 produced by Access Data Corporation, ProDiscover version 7.0.0.3 produced by Technology Pathways Corporation, and X-Ways Forensics version 16.3 produced by X-Ways Software Technology AG.

I have mastered these standard computer forensic methodologies through my personal experience performing forensic work and through my completion of numerous courses and certifications related to computer forensic methodologies.

During the period of May 3, 2012 through June 4, 2012, TRC performed an analysis of the March 26, 2012 Report of Digital Forensic Analysis created by Stroz Friedberg.

Distinction of Media

The analysis in this case involved two categories of Media

In multiple locations throughout their report, Stroz Friedberg makes reference to the "Ceglia Media." This convenient oversimplification used to describe the collective of evidence that was examined, improperly implies that each item of evidence belong to and was under the control of, the Plaintiff Paul Ceglia. In actuality, the majority of items described in the report belonged to and were under the control of Paul's parents, Vera and Carmine Ceglia. The pedigree of a particular item of evidence is important to any discussion concerning the facts surrounding that item. As such, a clear label should be provided when evidence belonging to a particular person is described. If the examiners were unaware of the ownership of each item of evidence, this oversight is understandable, however, I will list this important fact to better allow the reader to understand the context of any evidence described.

Owner of Seagate Computer

Vera and Carmine Ceglia Owned Computer with Seagate Hard Drive

The Seagate Hard Drive referenced multiple times in the report was removed from an HP Pavilion computer that belonged to Vera and Carmine Ceglia, Paul's parents. This fact appears to have been overlooked in the report or unknown to the writer. While this oversight is understandable, the significance of this fact cannot be overstated. This item of evidence was not owned by the Plaintiff, was not used by the Plaintiff, and was not controlled by the Plaintiff, however this is only the location where a copy of the "low quality resolution" StreetFax Contract was found.

Best Evidence

The Seagate hard drive described on page 11 was imaged on two different dates (March 29, 2011 and July 15, 2011). The image that was created on July 15, 2011 would contain two types of data:

1. Potentially relevant evidence that was on the drive when it was imaged on March 29, 2011 and

2. Data added after March 29, 2011.

Logically, the image of the drive that was made on March 29, 2011 contained the potentially relevant evidence made closes to the events in question and should be used for the examination. Any data added to or removed from the drive after March 29, 2011 would not be germane to specific events that occurred in 2003 and 2004. Therefore, unless a specific question is raised concerning data added to or removed from the drive between March 29, 2011 and July 15, 2011, the "Best Evidence" to examine would be the image created on March 29, 2011. Any data that is different between the two images, and was reported to have been on the drive before March 29, 2011, should alert the investigator that the earlier image would contain the "Best Evidence" and should be relied on instead of the later image.

Evidence of Malware

The Carmine and Vera Ceglia computer was infected

Due to the multiple reference of suspected fraudulent behavior referenced in the Report, it is noted that, conspicuously absent from the Stroz Friedberg Report was any mention that they checked for the presence of Malware. Malware (malicious software) includes computer viruses, worms, Trojan horses, spyware, adware, and rootkits.

Viruses – used for a program that has infected some executable software and when run causes the virus to spread. They may contain a payload that performs other actions, often malicious.

Trojan Horses – any program the invites the user to run it, concealing harmful or malicious code.

Rootkits – modifies the computer's operating system so that the malware is hidden from the user.

The images of the Seagate hard drive were scanned with malware detection software (Malwarebytes 1.61 and AVG 2012.0.2171) and the following malware were identified (this is not the complete list):

Virus Win32/Cryptor

Virus Win32/Heur

Virus Win32/DH

Virus Worm/Nachi.A

Virus I-Worm/Nuwar.U

Trojan.Drooper.Bravix.A

Trojan.Generic_c.VCZ

Trojan.Shutdowner

Trojan.Peed

Trojan.Downloader

Rootkit-Agent.CE

Rootkit.TDSS

It is reasonable to deduce from the results of the Malware Detection Software that the Seagate hard drive was infected with numerous malware files that potentially left the system open for compromise from an external source. A much greater and more time-consuming analysis of the evidence will be needed to specifically address the impact of each of these threats however, the following information is provided to list general details about each of the above listed malware:

- Virus Win32/Cryptor: Trojan that delivers a malicious payload and generally provides website redirection from search engine results, as well as disabling anti-virus software functionality.

- Virus Win32/Heur: AKA TrojanDropper:Win32/Dowque.A (Microsoft) is a generic detection for malicious files that are capable of installing other malware in the computer. (12) It drops other malware in the system folder and deletes its running copy using a batch file. Files usually dropped by TrojanDropper:Win32/Dowque.A are capable of hooking in processes or APIs. The following is a list of some of the malware families it may install:

  Win32/QQpass

  Win32/Qqhook

  Win32/Ceekat

Win32/Dowque

• Virus Win32/DH: AKA Generic.dx!bdhv (McAfee) is a Trojan detection that indicates a malicious payload that enumerates many system files and directories, Process attempts to call itself recursively and adds or modifies Internet Explorer cookies (15).

• Virus Worm/Nachi.A: This worm copies itself to the "Dllhost.exe" file on the system. It spreads by exploiting a RPC DCOM (Microsoft Security Bulletin MS03-026) and WebDAV (Microsoft Security Bulletin MS03-007) vulnerability. The worm creates the services RpcPatch and RpcTftpd. Other than attempting to spread to other computers in the same network, this worm also attempts to connect Microsoft's Windows Update in order to download security patches. If the system was infected in the year 2003 (the primary year of infection), the worm will self-remove and delete the installed services following the first system restart when the system date is 2004. This virus was widespread. (1,2,3)

• Virus I-Worm/Nuwar.U: Storm Worm, or Win32/Nuwar, refers to a family of Trojan droppers that install a distributed peer-to-peer (P2P) downloader Trojan. This downloader Trojan in turn downloads a copy of the email worm component of Storm Worm. Storm Worm uses advanced stealth techniques in order to hide its files and associated registry modifications. Hence, it is unlikely that users could easily ascertain the presence of the Trojan on the infected computer. To obtain addresses in order to spread, Storm Worm enumerates the first 30000 files under 122k on all fixed and remote drives. The worm will spoof the sender address to be a randomly chosen name from a list from the yahoo.com domain. The message body will be blank (4). The subject line of the email generally uses fictitious and incendiary topics, for example:

USA Declares War on Iran

230 dead as storm batters Europe

USA Missle Strike: Iran War just have started

Naked teens attack home director

The email includes an executable (.EXE) attachment which may use on of the following file names:

More.exe

Read More.exe

Click Here.exe

- Trojan.Drooper.Bravix.A: AKA FakeAlert-AP (McAfee) AKA TrojanDownloader:Win32/Renos (Microsoft) automatically downloads potentially unwanted software such as SpySheriff, SpyAxe, SpyFalcon, SpyDawn, SpywareStrike, and other similarly named programs. These programs typically present erroneous warnings claiming the system is infected with spyware and offer to remove the alleged spyware for a fee. In some cases, the programs may also cause system instability. (5,6)

- Trojan.Generic_c.VCZ: Generic Trojan that slows down system processing, produces unwanted pop ups, potentially modified wallpapers, places system information and private at risk for being captured by the malicious actor behind the attack. This virus is typically spread via email attachments, messaging software, freeware or infected web sites.

- Trojan.Shutdowner – Generic identifier for malware/Trojans that deliver a malicious payload and generally provide website redirection or the payload code is used to monitor and modify web search queries and display its own online advertisements (14). See Trojan:Win32/Bamital.G (Microsoft)

or Mal/Mdrop-Fam (Sophos). Typically is accompanied by modification to the Hosts file.

- Trojan.Peed – A variation of the "Storm Worm" identified by BitDefender, also several variations have different methods of attack in the Trojan.Peed family. They generally range from a Trojan that steals credentials and damages user's computer. It also downloads and executes files from a remote server (10) to a chat client worm with backdoor Trojan functionality (11).

- Trojan.Downloader – A generic detection name used to identify malicious software programs that share the primary functionality of downloading content. (13)

The content that is downloaded varies from one example to the next. It may comprise of, but need not be limited to, the following items:

Configuration/command information

Miscellaneous files

Other threats or security risks, such as components related to pay per install operations

Misleading Applications

Secondary components of, or upgrades to, the existing attack

- Rootkit.TDSS – AKA Rootkit.Win32.TDSS AKA Alureon.

A rootkit is a program or a program kit that hides the presence of malware in the system (9). The placement of a rootkit is not normally something that is undertaken by a user with their own system and is generally an indicator of malicious activity.

According to the EC-Council, the primary purpose of a rootkit is to allow an attacker repeated, unregulated, and undetected access to a compromised system. A rootkit may be a bundle of tools such as a network sniffer or log-cleaning scripts or utilities. Rootkits can crack passwords at the administrator level as well as exploit a system's vulnerabilities. To facilitate continued access, a rootkit may disable auditing, edit event logs, and circumvent intrusion detection systems. The rootkit hides it presence by erasing any traces after each execution, which makes it difficult to identify a rootkit in action. It can be more easily identified when it is passive. Rootkits can be removed by booting on an alternate drive. The rootkit hides files in particular folders and does not spread like viruses do. (16)

A rootkit for Windows systems is a program that penetrates into the system and intercepts the system functions (Windows API). It can effectively hide its presence by intercepting and modifying low-level API functions. Moreover it can hide the presence of particular processes, folders, files and registry keys. Some rootkits install its own drivers and services in the system (they also remain "invisible"). (9)

The TDSS/TDL/Alureon MBR rootkit Trojan is a particularly malicious program. When your computer is infected with the Trojan, the Master Boot Record (MBR) is altered to ensure that the Trojan will even survive a complete format of the hard drive. Once your computer is infected, the Trojan sends information from your computer to a criminal enterprise. The types of information that are stolen are account ids and passwords…credit card information (PIN numbers, expiration dates and card numbers) and banking information (account numbers, passwords, etc.). (7)

There are two ways that this rootkit can spread as a self-propagating mechanism. The first is by infecting removable media drives with a file that gets executed each time a computer connects to the device. The second method is to spread over local area networks by creating a rogue DHCP

server and waiting for attached machines to request an IP address. When the malware finds a request, it responds with a valid address on the LAN and an address to a malicious DNS server under the control of the rootkit authors. The DNS server then redirects the targeted machine to malicious webpages. (8)

Sources:

1. http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=100559

2. http://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/W32~Nachi-A/detailed-analysis.aspx

3. http://www.symantec.com/security_response/writeup.jsp?docid=2003-081815-2308-99&tabid=2

4. http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Storm+Worm

5. http://home.mcafee.com/virusinfo/virusprofile.aspx?key=776228#none

6. http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=TrojanDownloader%3aWin32%2fRenos

7. http://www.utdallas.edu/infosecurity/Fix_Instructions.html

8. http://techtalk.seattle.gov/2011/06/07/notorious-rootkit-tdss-also-goes-by-the-names-alureon-and-tdl4-gets-self-propagation-powers/ or http://www.theregister.co.uk/2011/06/03/tdss_self_propagation_powers/

9. http://support.kaspersky.com/faq/?qid=208283366

10. http://www.microsoft.com/security/portal/threat/Encyclopedia/Entry.aspx?Name=Trojan%3AWin32%2FOmexo.C

11. http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Backdoor%3AWin32%2FSdbot.ZD

12. http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=TrojanDropper%3aWin32%2fDowque.A

13. http://www.symantec.com/security_response/writeup.jsp?docid=2003-011710-3138-99

14. http://www.microsoft.com/security/portal/threat/Encyclopedia/Entry.aspx?Name=Trojan%3AWin32%2FBamital.G

15. http://home.mcafee.com/virusinfo/virusprofile.aspx?key=896090#none

16. Press, EC-Council. (2009). Ethical hacking and countermeasures, attack phases. Clifton Park, NY: Course Technology Ptr.

Zuckerberg's Capabilities

Allegation of Zuckerberg hacking a computer is not far-fetched

The report states, "It would be extraordinarily difficult for an individual, even a person with significant technical expertise, to 'plant' the StreetFax Emails on the Ceglia Media or Sidley Austin's servers."

In an article for The Harvard Crimson, titled "Hot or Not? Website Briefly Judges Looks" (dated Nov 4, 2003, by Bari M. Schwartz), Mark Zuckerberg's exploits while developing the "Harvard Face Mash" site are detailed. Quotes are included from Zuckerberg's "Online Diary" that describes the process he used to "hack" into Harvard's dormitory photo ID records. Zuckerberg called the hacking "Child's play" and even admits "I'm a little intoxicated, not gonna lie" while hacking into the "houses" and stealing the photos.

For someone who considers hacking into Harvard's computer files to steal photo ID records, while intoxicated, to be "child's play," the idea that he could "plant" the StreetFax Emails is not that farfetched. Additionally, it is widely reported that in 2004, Zuckerberg hacked into the email accounts of two Harvard Crimson reporters using data obtained from TheFacebook.com's logs.

It should be noted that these examples of hacking by Mr. Zuckerberg were conducted "remotely"—he was not physically present at the locations where the Photo ID files were stored or the email servers for the Harvard Crimson were located. As has been shown, Mr. Zuckerberg has the technical expertise to gain access to computers without physically touching or being in the same location as the computer. As will be discussed, Malware (viruses, Trojans, and rootkits) found on the Plaintiff's parent's computer are tools that can be used by a hacker to gain and retain remote access to a computer for purposes

including theft of information, disabling of the system, or to take remote control of the computer.

The report describes in great detail many of the items that would have to take place in order to "plant" the emails. An alternate theory as to how the emails could have been "planted" on the Seagate hard drive and the Sidley Austin email server was tested and validated as possible.

Alternate method by which the emails appear to have been sent from the computer

As opposed to actually hacking into Ceglia's parent's computer to send the emails, someone could have simply accessed the Adelphia.net's email server using the logon credentials for Carmine Ceglia. Carmine Ceglia, like many other Internet users, admits that he used the same username and password for multiple website logins including for his account on the StreetFax server that Mr. Zuckerberg had full access to. Someone attempting "plant" the emails could have sent the emails from a computer via a web browser, logged in to Adephia.net email server, using Carmine Ceglia's username and password. Then, the emails would be in the "Sent Items" folder on the email server. The next time that Carmine or Vera Ceglia logged into Adephia.net to check or send their email using Outlook Express, the "Sent Items" folder would synchronize the email folder on the server with the email client, Outlook Express, on their computer. Now, the computer would have the email messages (in the Sent Items folder) of the Outlook Express DBX file, and it would appear that the messages were sent from that computer.

This theory was tested and validated and worked as described. A Gmail.com email account was used in place of the Adephia.net email server because the company is no longer offering email service. The client computer that was used was running Windows XP and Outlook Express 6. An email (with an attachment) was sent from a web browser utilizing a test Gmail.com account. When Outlook Express was later synchronized with Gmail, the sent email (with the attachment) was copied into the Sent Items folder within Outlook Express on the computer. This is one possibility to describe how the emails could have been sent to Mr. Kole and how they could have been placed onto Ceglia's parent's computer.

The Internet header information would all appear legitimate, because it is. I did not have access to the Email produced by Sidley Austin for comparison or the Adelphia.net account records for verification. The report states that the originating IP address of the emails was 24.53.222.222, however any computer on the Adelphia.net network would have received a temporary (dynamic) IP address from within the pool of all available addresses belonging to Adelpha.net.

Vera Ceglia's Outlook Express Account

Email contents of Vera Ceglia's email account is atypical

The Outlook Express Email account referenced on Stroz Report pages 11-16 did not belong to Paul Ceglia; it belonged to Vera Ceglia, Paul's mother. As is listed in the Report, the Plaintiff had access to multiple web based email systems including Yahoo, Gmail, and MSN, each of which allows for an attachment to be sent. The question remains, why would the Plaintiff use his mother's email account to send an email to his attorney if he could have used any of his web based email accounts?

The report (page 12) mentions the two emails that are contained in the "Sent Items.dbx" file. What the report fails to mention is that the entire contents of the Sent Items.dbx consists of only 5 sent emails:

1. "earrings"
2. "postage"
3. "REFUND"
4. "page 1 of 2 for Streetfax contract w mark"
5. "2 of 2 for streetfax contract"

It is highly unusual that so few "Sent" messages would be found on a computer and specifically, that two of these emails work to disprove the Plaintiff's contentions, yet they are the ones that were retained.

Additionally, as is evidenced by the lack of email in the Outlook Express file, this program was not the main email utility that the Plaintiff's parents used to check email on their computer, they also used a web based email service. Again, the question remains, why would the Plaintiff use his mother's

Outlook Express email application account to send an email to his attorney if he could have used any of his web based email accounts?

Poor Quality of Email Attachments

The TIFF files attached to the StreetFax email sent to Jim Kole are alleged by Stroz Friedberg to have resulted from scanning. Therefore, somewhere, at some time, the two pieces of paper existed containing the content that is now reflected in the scan must have existed.

The metadata of the TIFF files that were attached to the StreetFax emails that were sent to Jim Kole on March 3, 2004 show that the dimensions of the scanned documents were approximately 2.4 x 3.2 inches (480 x 646 pixels at 200 dpi for Scan0001.tif and 480 x 657 pixels at 200 dpi for Scan0002.tif; both in 24bit color mode).

For further explanation…200 dpi refers to 200 dots (pixels) per inch; when you divide 480 pixels by 200 dpi, you get 2.4 inches –this is the width of the scanned pages. When you divide 646 pixels by 200 dpi, you get 3.23 inches – this is the height of Scan0001.tif . When you divide 657 pixels by 200 dpi, you get 3.285 inches –this is the height of Scan0002.tif.

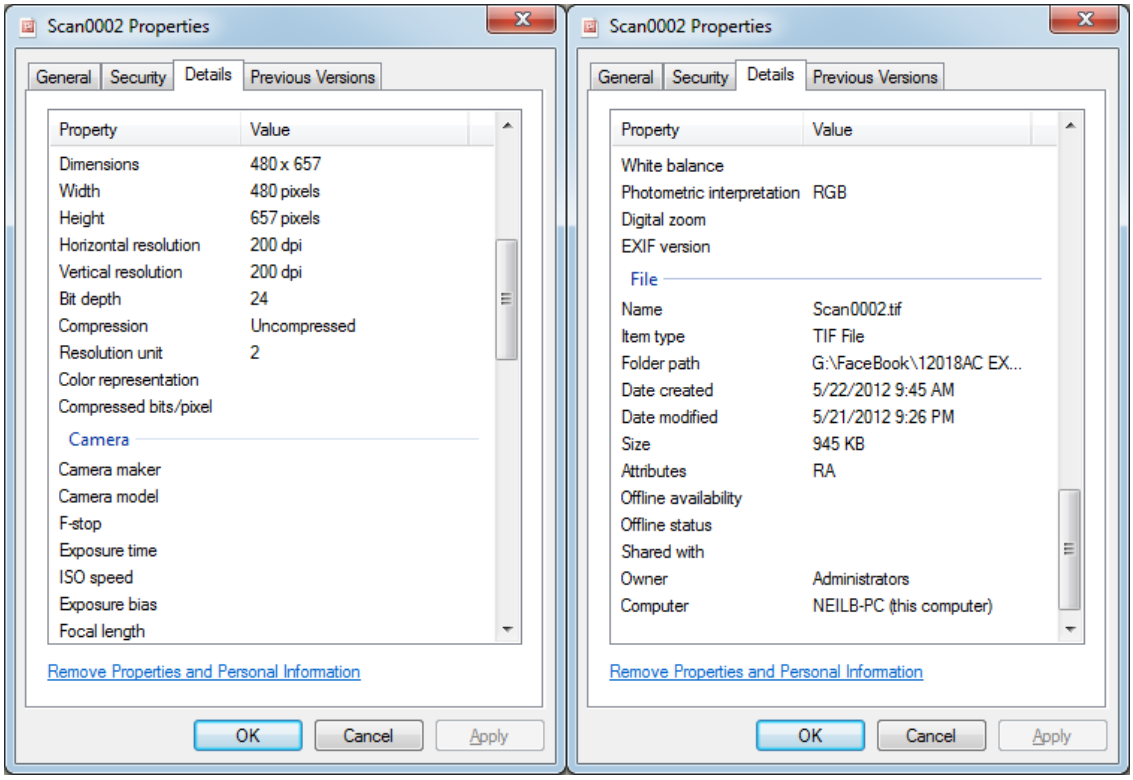
In order to recreate these same values, I started with an 8.5 x 11 inch standard page of paper and then created a copy of the page, reducing the size of the copy to 30% of the original. This copied (and reduced) page was then placed on a scanner with the scan area set to 2.4 x 3.2 inches and scanned at 200 dpi, in color mode. The resulting file was 945 KB, the same general size of Scann0001.tif (923 KB) and exactly the same size as Scan0002.tif (945 KB), please see the Properties information below.

The Stroz Friedberg Report notes on Page 14, "The TIFF image attachments appear to be scanned documents and are of low-quality resolution." In fact, these documents appear to be 30% the size of a typical 8.5 x 11 inch page of paper. Please see the image of "Test Scan Doc.tif" below and compare it to

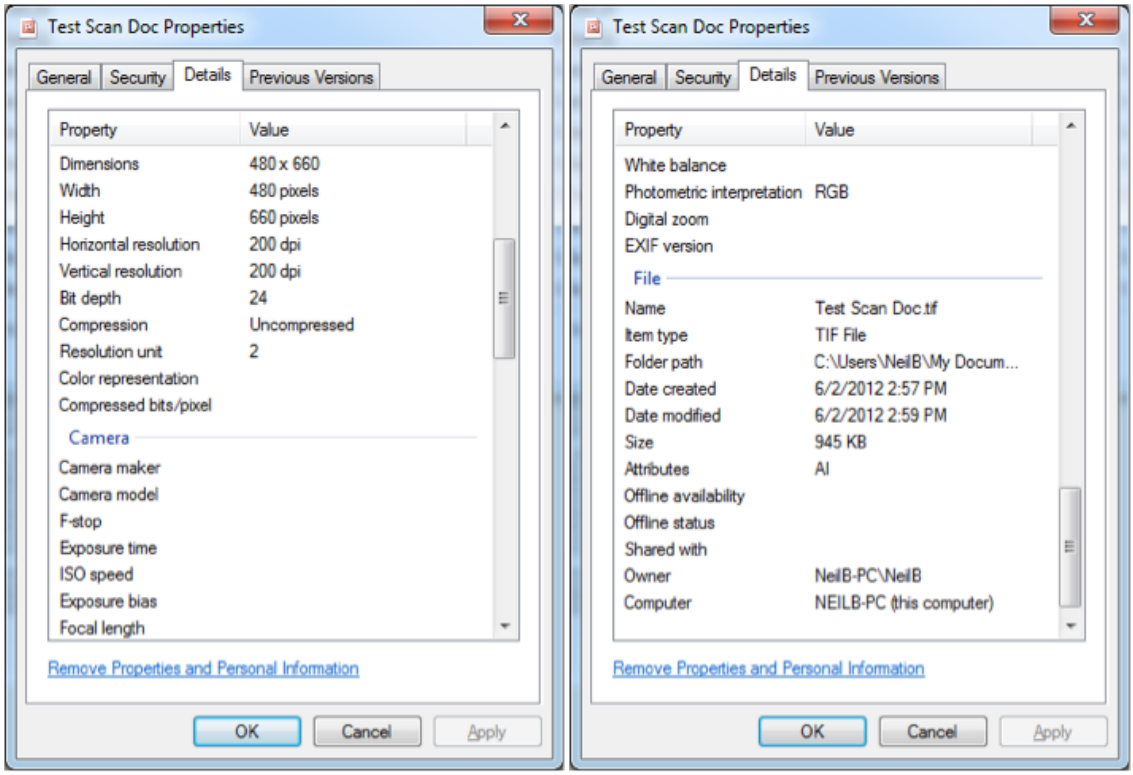
Exhibits F and H of the Stroz Friedberg Report; each of the images has the same "low quality resolution."

Since scanners do not automatically reduced the size of files they copy, to a point of making them illegible, why would the Plaintiff scan a file in such a manner if the point of the email was for him to receive assistance from his attorney? If the Plaintiff was interested in receiving the assistance of his attorney, wouldn't he have simply scanned the documents at their normal size and then emailed them to the attorney? It is interesting to note, attorneys for the Plaintiff have hired a Digital Image Expert in this case and he reported that the quality of the Scan0001.tif and Scan0002.tif files are too low quality to accurately examine.

SCAN 0002.TIF PROPERTIES



TEST SCAN PROPERTIES



Test Scan Doc.tif


STREET FAX

Backdating

Alternate Explanations

The report list instances of the Seagate hard drive being backdated. The only possible explanation that is offered is that "the system clock of the computer that contained the Seagate hard drive was backdated." There are other reasonable explanations as to how the clock could have been altered that were not caused by intentional actions of the Plaintiff.

The time on the computer is retained by the CMOS battery while the computer is turned off and unplugged. If a computer has been unplugged for a long period of time, it is possible for the battery to drain and the CMOS clock to give erroneous readings. This CMOS time (whether right or wrong) is what gets reported to the Windows Operating System when the computer is restarted. On a test laptop that had been unplugged for over 1 year, when it was turned on (May 30, 2012 at 12:09 P.M.) the computer's clock showed Nov 20, 2003 at 10:03 A.M. This laptop had the correct time setting the last time it was used. In summary, the discharge of the CMOS battery could have caused the computer's clock to change its time after it was powered on after being unplugged for a long period of time.

Additionally, the large number of viruses, Trojans, and Rootkit files found on the computer show that it could have be manipulate by someone other than the Plaintiff via an Internet connection.

Time Zone Stamp

Explanations for anomalies

The word "anomaly" is a commonly used term in computer forensics. Anomaly is used to denote an unexpected finding. It is a neutral word that does not, in and of itself, mean fraud.

On Page 20 of the Report, Note 9 at the bottom of the page states the following:

> "The Sidley Austin server named mail02.sidley appears to be set to the Central time zone, as the time it appended to this Internet header (9:38:01 a.m.) is approximately one hour earlier than the time appended by the Adelphia server (10:37:10 p.m.), which resided in the Eastern time zone. However, the offset indicates that the time zone is set to Eastern time. The server time and time zone are separate fields that can be set independently. Thus, the likely explanation is that while the server time was correctly set and reflects the actual time in the Central time zone, the time zone setting was incorrectly set to Eastern time."

Please note it is assumed that the Report meant to have stated 10:37:10 a.m.

On Page 21 of the Report, Note 10 at the bottom of the page states, "The server mail01.sidley also appears to have an incorrect time zone setting."

Both of the above notes are remarkable because on Page 27 of the Report, it is highlighted that "The Purported Emails Contain the Wrong Time Zone Stamps." The dialogue continues, "all but one of the 27 purported emails contain the '-0400' time zone stamp for Eastern Daylight Time, including all of the purported emails supposedly sent between October 26, 2003 and April 4, 2004." Continuing, "There is no place in the Continental United States

from which an email could have been sent with the '-0400' time zone stamp during this time period using a computer with an accurate and properly set system clock."

In this regard, the Report contradicts itself. On Pages 20 and 21, when a Time Zone Stamp irregularity works against them, the Report brushes off the value of the data, however, on Pages 27 and 28, when the Time Zone Stamp anomaly works in their favor, the Report infers the emails could not be authentic because of this same Time Zone Stamp variance.

Experiment recreates time zone anomaly

I conducted a test using Gmail.com to see how this web based email system would report the time of an email that was checked on a computer that was set to the correct time, however the time zone was incorrectly set (to Mountain Time Zone).

> From: nbroom@trcglobal.com Neil Broom
>
> To:
>
> Date: Sun, 3 Jun 2012 01:37:22 -0600
>
> Subject: Incorrect Time Zone
>
> I am sending this email at 12:37 a.m (in L.A.) on a computer that shows that time, however the computer incorrectly shows in the Mountain Time Zone.
>
> Neil Broom

I then corrected the time zone setting (to Pacific Time Zone) and sent a second test email using Gmail.com. Please note that I restarted the Internet Explorer Browser and Signed In to Gmail.com again after I changed the time zone setting.

> From: nbroom@trcglobal.com Neil Broom
>
> To:
>
> Date: Sun, 3 Jun 2012 00:41:29 -0700
>
> Subject: Correct Time Zone
>
> I am sending this email at 12:41 a.m (in L.A.) on a computer that shows that time and the computer correctly shows in the Pacific Time Zone.
>
> Neil Broom

As you can see, the Time Zone Stamp in the email message that was read (from the Gmail.com webpage) on a computer, with the correct time, but configured with the incorrect time zone (one hour before), showed a "-0600" when it should have showed "-0700." This is the same behavior displayed in the emails on Pages 27 and 28 of the Report. There is no way to determine if MSN functioned in this same fashion in 2003 and 2004, however, this test proved that an inaccurate Time Zone Stamp is not necessarily evidence of a fraudulently created email message.

The following quote can be found at the bottom of page 28 of the Stroz Report, "Put simply, Mr. Ceglia's purported emails dated between October 26, 2003 and April 4, 2004 display the time zone stamp reflecting Eastern Daylight Time. This would not be possible if the purported emails were authentic, as Eastern Standard Time was in effect at that time." The above test shows that the possibility does exist for authentic emails to have the wrong time stamp, especially if the computer was set with the incorrect time zone. It should be noted that the Plaintiff, Paul Ceglia, maintains property in Nova Scotia, Canada, which is in the Atlantic Time Zone (1 hour less than the Eastern Time Zone) and therefore it can reasonably be assumed that the computer could have been set to the Atlantic Time Zone and later, when brought back to the U.S., only the clock was adjusted and not the time zone.

The U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, NIJ Special Report, "Investigations Involving the Internet and Computer Networks" (Jan 2007) contains the following relevant quotes:

Page 2, "Server and computer clocks may not be accurate or set to the local time zone. The investigator should seek other information to confirm the accuracy of time and date stamps."

Page 21, "CAUTION: If the date and time associated with the e-mail are important to the investigation, consider that this 'Received' time recorded in the e-mail header comes from the e-mail server and may not be accurate."

Page 22, Under the heading of "Time Stamping":

> "Investigators should be aware that when examining e-mail headers, times may not be consistent. Date and time stamps related to the header should be scrutinized as these times may be added by different servers in different parts of the world and different time zones and may not be consistent. In addition, clocks built into computer systems and powered by batteries—especially those on personal computers—may not always be accurately set or may not keep time correctly, resulting in the wrong time. Special consideration should be given to looking for time zone information related to the time."

These multiple warnings, listed in this U.S Department of Justice Publication, concerning the inaccuracy of time in a computer forensics investigation, highlight the fact that Time and Time Zone Stamp irregularities do not necessarily mean fraud, as is alluded to in the Report. There can be other explanations for the anomalies, if the investigator keeps an open mind.

Formatting Differences

The report makes reference to the first page of "Work for Hire ContractMZ.doc" and states that the spacing is "unusual." One possible explanation that does not appear to have been examined is that the author of the document could have altered the spacing of the document at the time the document was originally created (or altered from a template) so that the formatting for page two would remain constant even though additional language had to be added to page 1 to fully describe both the StreetFax and The Face Book projects.

Email is a Two-Party Communication

Based on the evidence in the Report, the email communications that were copied and pasted in Word Documents by the Plaintiff are in question. These presented copies of the emails are only one half of the conversations. The other half of the conversations and therefore proof of their validity can be found in the email records of Mr. Zuckerberg during the timeframe in question. Due to other litigation that was in process, Mr. Zuckerberg's emails were preserved and a review of those preserved emails could help prove or refute the validity of the Plaintiff's email evidence.

Re-Installation of the Windows Operating System

The Report states that the Windows Operating System on the Seagate hard drive was reinstalled on at least two occasions. This hard drive was not used by the Plaintiff and was not in his control – the hard drive belonged to his parents. The reinstallation of the Operating System that occurred on the hard drive was done by Paul's father, Carmine Ceglia because the computer was not working properly.

As was mentioned in the Report, this hard drive was forensically imaged on March 29, 2011. Activity occurring on the hard drive after that date is not relevant to the activities that occurred in 2003-2004 due to the fact that there is no way the hard drive could possibly reveal any additional evidence from its past, by examining a later forensics image.

The Stroz Report mentions Google Searches for "when did windows xp release" and "look up the date a hp computer was made" and Stroz states the searches "may be related to this backdating and reinstallation." These searches could also have been done by someone trying to figure out if their computer was still within its warranty period. All parties agree that the Seagate hard drive has major issues with date entries; we contend that these issues could have been caused by a problem with the CMOS battery because the computer was unplugged for a long period of time or because of the viruses, Trojans, and Rootkits that were found on the drive. It is my opinion that none of the dates on this hard drive should be trusted without external verification and that any potential evidence discovered that relies on date evidence from the hard drive should be circumspect.

Improper Section Title

Street Fax Contract was not found on two different Ceglia hard drives

The section title "The StreetFax Contract Was Found on Two Different Ceglia Hard Drives" is used on page 11 of the report. This statement is factually incorrect –the report describes a single Seagate hard drive that was imaged at two separate points in time (March 29, 2011 and July 15, 2011) and not two different hard drives. The use of the statement "Found on Two Different Ceglia Hard Drives" is used to bolster the legitimacy of potentially relevant evidence discovered. As demonstrated by footnote 4 on page 11, the writer of the report knew this fact and yet purposefully chose to exaggerate the possible validity of the potentially relevant evidence by stating it comes from "Two Different Hard Drives." Footnote 4 reads, "The Forensic Image Created by Plaintiff's Expert was created on March 29, 2011 and subsequently preserved by Stroz Friedberg on July 18, 2011. The Seagate Hard Drive itself continued to be used after March 29, 2011 and was imaged by Stroz Friedberg on July 15, 2011."

Production from Sidley Austin

Based on information in the Stroz Friedberg Report, they obtained native format copies of the StreetFax emails pursuant to a subpoena authorized by the Court. Attorney for the Plaintiff, Dean Boland has confirmed to me that he has not received native format copies of these emails and I am unable to confirm any of the information on pages 18 – 22 of the Report without them.

I hereby declare under penalty of perjury and pursuant to 28 U.S.C. 1746 and under the laws of the United States that the following is true and correct:

DATED: June 4, 2012

Neil Broom