Effectively Using Cutting-Edge Computer Forensics in Non-Compete and Trade-Secret Cases

Daniel C. Gerhan
Boston Scientific Corp
Arden Hills

Scott Larson
Larson Security
Minneapolis

Joel P. Schroeder
Best & Flanagan LLP
Minneapolis

Lucas Woodland
Seneca Security LLC
River Falls

Employment Law Institute – May 2017

Minnesota CLE's Copyright Policy

Minnesota Continuing Legal Education wants practitioners to make the best use of these written materials but must also protect its copyright. If you wish to copy and use our CLE materials, you must first obtain permission from Minnesota CLE. Call us at 800-759-8840 or 651-227-8266 for more information. If you have any questions about our policy or want permission to make copies, do not hesitate to contact Minnesota CLE.

All authorized copies must reflect Minnesota CLE's notice of copyright.

MINNESOTA CLE is Self-Supporting

A not for profit 501(c)3 corporation, Minnesota CLE is entirely self-supporting. It receives no subsidy from State Bar dues or from any other source. The only source of support is revenue from enrollment fees that registrants pay to attend Minnesota CLE programs and from amounts paid for Minnesota CLE books, supplements and digital products.

Computer Forensics in Non-Compete and Trade-Secret Cases

Daniel Gerhan, Director & Senior Litigation Counsel, Boston Scientific Corporation
Scott Larson, President, Larson Security
Joel Schroeder, Partner, Best & Flanagan LLP
Lucas Woodland, President, Seneca Security

Upper Midwest Employment Law Institute, St. Paul, Minnesota
May 23, 2017

****

"To keep your secret is wisdom, but to expect others to keep it is folly."
--Samuel Johnson

Non-compete and trade-secret cases can be complex and difficult to litigate. They are frequently fast-paced; time-consuming; and expensive. Smoking guns are rare and circumstantial evidence is common. Computer or digital forensics, however, can sometimes make all the difference in these cases. If not providing a smoking gun, computer forensics can often provide the evidence necessary to establish that a non-compete should be enforced or that a former employee has misappropriated trade secrets.

When an employee leaves her employer and accepts a job at a competitor, it is often the case that he or she does not leave empty-handed. Mostly gone are the days when employees snuck out in the middle of the night with a brief case full of company trade secrets (although that still happens). A much more common scenario is the departing employee siphoning company trade secrets using a computer or other device—such as emailing company trade secrets from the company email account to another email account; emailing them to a Gmail or Yahoo! account; uploading them to a cloud account; printing them off; or taking photographs of them with a smartphone.

These materials and our panel presentation will provide an overview of computer forensics, including common sources of forensic evidence and the type of evidence that can be discovered by computer forensics; examples of courts denying or granting requests for forensic imaging and analysis; tactical considerations when securing forensic imaging and analysis; best practices for expert affidavits; presenting forensic evidence to the jury or jury; and tips for working with computer forensics experts.

I. WHAT IS COMPUTER FORENSICS?

Computer or digital forensics is the application of investigative and analytical techniques to gather and preserve evidence from computing devices in a way that is suitable for presentation in court. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to discover

what happened on the computing device and who (or what) was responsible for what happened.

Sound forensic analysis begins with the preservation of evidence. Preservation in a forensically sound manner involves making a bit-stream copy—or mirror image—of the computing device. Courts have described "mirror images" or "forensic images" as "a forensic duplicate, which replicates bit for bit, sector for sector, all allocated and unallocated space…on a computer hard drive." *Balboa Threadworks, Inc. v. Stucky*, 2006 WL 763668, *3 (D. Kan. Mar. 24, 2006).

Forensic imaging is accomplished by using "write-blocking" hardware or software that copies the subject digital media without altering or deleting any original data. *See N.H. Ball Bearings, Inc. v. Jackson*, 969 A.2d 351, 356 (N.H. 2009) (forensic images allow "investigation of past use without altering the original evidence"). This forensic bit-stream copy includes not only the programs and file content visible to an average user, but also system logs, temporary files, previously deleted content and other latent data that may be important to any determination about how confidential information and trade secrets may have been handled. Forensically sound methods also involve obtaining a mathematically unique figure known as a "hash value" for each forensic data copy. This hash value serves as an electronic "fingerprint" that can verify the authenticity of any forensic copies made from the original data.

Forensic analysis uses various analytical techniques to try and identify any activity possibly related to the theft of confidential information or trade secrets (or the incident in question). Forensic analysis typically involves creating initial reports that list active files, previously deleted files, Internet surfing activity, recently accessed files, and inserted removable devices. Forensic analysis also may include, but is not limited to, (1) keyword searches to look for particular active or deleted files, or (2) examining the device for file fragments in spare sectors known as "free" or "unallocated" space. Through these and other analytical techniques, forensic analysis provides a more complete understanding of how or if confidential information and trade secrets might have been transferred unlawfully.

II. COMMON SOURCES OF DIGITAL EVIDENCE

When beginning a forensic analysis, it is important to consider what type of devices the former employee (or other target of an investigation) might have used. The most common types of devices are: (a) computers, (b) mobile telephones and devices, (c) cloud storage, and (d) removable devices.

a. Computers

Computers (desktop computers, laptops, and servers) are the mainline sources of digital evidence. A computer and its components are frequently the cornerstone of evidence in trade-secret investigations. Potential sources of evidence include: the hardware, software, documents, photos, scanned images, e-mail and attachments,

databases, Internet browsing history, event logs, data stored on external devices, and identifying information associated with the computer system.

On computers there are three main areas of evidence: (1) active files, (2) deleted files and (3) unallocated space.

Active files are generally accessible to the computer operating system and user and include system and program files, as well as user-created files such as word-processing documents, spreadsheets, and PowerPoint presentations. Reports of active files are important because they list files or file paths that continue to reside on the computer(s), server(s), and other digital media.

When a user highlights an active file and hits the "delete" key on a Microsoft Windows computer, that file is assigned to the Recycle Bin but it is treated as an "active" file as described above. When the file is "double deleted" and removed from the Recycle Bin, the File Allocation Table (or "FAT") or Master File Table (or "MFT") ceases to reference the physical sectors containing data for that file. Instead, the FAT or MFT indicates that the physical sectors previously used by that file are now available for the recording of new data. A deleted-files report can show relevant files that were stored on the computer(s), server(s), and other digital media used by the custodian, but have since been deleted.

The unallocated and file-slack portions of a hard drive can be reviewed for fragments responsive to keywords or data-carving techniques. These areas may contain deleted files, unsaved data from web browsing, and temporarily cached files or e-mails that the user has opened but not saved. Additionally, analysis of unallocated space for patterns of repeating characters can indicate the use of a wiping utility or methodology.

b. Mobile Telephones and Devices

Mobile devices are another major source of digital evidence. Most commonly mobile devices refer to cellular/smart phones, but also include tablet computers, GPS devices and personal digital assistants (or "PDAs").

In addition to enabling voice communications, cellular/smartphones now offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. A cellular/smartphone usually includes a "call log," which records the telephone number, date, and time of calls made to and from the phone. Additionally, tablets and smart telephones run applications, like computer software, giving them many of the same capabilities as personal computers.

For example, tablet users can work with word-processing documents, spreadsheets, and presentations, save the file to the cloud, and then access the file on their computer or laptop. Most smartphones and tablets also include GPS technology for determining the location of the device.

c. Cloud Storage

The cloud is another major source of evidence and one that has become much more commonplace in forensic investigations. Cloud computing is Internet-based and is a method for sharing resources, processing and storage. Some of the common cloud storage options are Apple iCloud, Dropbox, Microsoft OneDrive and Google Drive. With these cloud-storage options, files and data are created on one device and then saved and synchronized across any number of other devices determined by the user. Cloud storage is often used as a collaboration tool by companies because the owner can share folder and files with any other person. Once the file or folder is shared it also synchronizes across the other users' devices as well.

d. Removable Devices

Many removable or external devices are also known as "USB" devices because they use a common "Universal Serial Bus" protocol to interface with the computer. When a USB device is attached to a computer, the operating system pulls data from the device and, within the registry, records values or codes that represent information like the vendor ID, product ID (and revision or version number), and the specific serial number of each USB device. If no serial number is present, the Microsoft Windows operating system itself will generally create a unique value within the serial number field. Removable devices have the same types of data as computers, with active files, deleted files and unallocated-space.

On Microsoft Windows computers, the "registry" is a database on a hard drive that stores settings and options for the operating system. Among its various functions, the registry records what types of external or "removable devices" have been attached to a computer and when. A registry entry for an external device often shows a "last written" time, indicating when the registry entry for that device was last updated and, therefore, when the device was last attached to the computer.

III. LIMITATIONS IN COLLECTING DIGITAL EVIDENCE

There are several limitations in collecting digital evidence. The first is the volatility of the data. Volatile data is the data stored within this memory type, such as random access memory (or "RAM"), which can be lost completely when a computer or mobile device loses its power source or is turned off. For example, if a file is created but not saved to the hard drive and the computer loses power, that file can be lost and not recovered.

Another limitation in collecting digital evidence is the increase use of encryption. Encryption is the process of encoding data to prevent unauthorized access. If digital evidence is collected but encrypted, the forensic expert will not be able to access the data unless he or she has the key or passphrase to decrypt the data. While there are some brute force methods available to defeat the encryption (such as "jailbreaking" a device), many of these methods require extensive time and incur high costs. When collecting computers, tablets and smartphones, it is now crucial to also collect the password or pin, because without the key, the data is inaccessible. The Apple iPhone encryption was the focus of attention in the recent San Bernadino case where the FBI received help from the cell phone forensic company Cellebrite. Cellebrite was able to decrypt the phone, but it was an older iPhone 5C. If the iPhone had been a newer version, it is unlikely that it would have been decrypted.

The volume of data is another limitation to consider for any case requiring computer forensics. The Apple iPhone 7 now comes with 256 gigabytes of storage and some retailers sell 10 terabyte hard drives. For reference, it is estimated that 85,899,345 pages of Word documents would fill one terabyte of storage. The storage capacity of computing devices greatly increases the time and cost associated with the preservation of digital evidence. The increased storage capacity of computers and storage devices has led to the increased use of targeted preservations where the forensic expert will preserve specific parts of the storage device that may contain data relevant to a legal investigation.

IV. SPOLIATION OF DIGITAL EVIDENCE

Because one who misappropriates trade secrets may also look for ways to cover up his or her conduct, spoliation of evidence should be top of mind when dealing with digital evidence. In general, spoliation occurs when a party alters, hides, or destroys evidence that is relevant to a civil or criminal case**.** There are many ways that spoliation can occur and it is important to know how to determine if it occurred.

Mass deletions occur when the custodian deletes numerous files and/or folders at the same time. In the Microsoft Windows operating system, the Recycle Bin is a holding area for files and folders that have been deleted by the user. A hidden system file within the Recycling Bin (which is referred to as INF02), contains a list of the deleted files, including the date, time and the path of deleted files that have been transferred to the Recycle Bin until it is emptied. The INF02 record is used by the operating system to undelete a file if a user later changes his/her mind. The "last modified" time of the INF02 file shows when the last file was added to the Recycle Bin, or when the Recycle Bin was emptied. The INF02 records may show files that were deleted and if a large number of files or entire directories were deleted at once.

Data wiping is another way in which digital evidence is destroyed. To wipe a hard drive or other storage device, a random or repeated set of characters is written to the entire hard drive effectively deleting or wiping all of the files and folders from the storage device. Wiping tools can also be used to wipe or erase specific files or portions

of the storage device. Analysis of unallocated space for patterns of repeating characters can indicate the use of a wiping utility or methodology.

V. THE TYPE OF INFORMATION THAT CAN BE DISCOVERED BY A COMPUTER FORENSICS EXPERT

Forensic analysis of electronic devices can be fertile ground for evidence in non-compete, trade-secret and other unfair-competition cases. As one court explained, forensic analysis can result in a veritable treasure trove of information:

> Analysis of the forensic image with forensic software allows an investigator to determine what peripheral devices have been connected to the device, what a user accessed, what has been stored on the device, and when it was last accessed or modified. Because deleted files are not actually erased from storage media, analysts are able to determine both current and deleted files so long as the latter have not been completely overwritten with new data.

N.H. Ball Bearings, 969 A.2d at 356.

When a computer forensic analyst is presented with a computer or other electronic device, he or she may search the image of that device for the following type of information:

- ✓ What other devices have been connected to the device;
- ✓ What user accessed the device;
- ✓ What has been stored on the device;
- ✓ When the device was last accessed;
- ✓ When data or documents on the device was last accessed or modified;
- ✓ What and when websites were visited; and
- ✓ With whom the user communicated.

VI. COURT ORDERS FOR FORENSIC IMAGING AND ANALYSIS

As described below in Section VII, parties should attempt to reach agreement on how or if electronic devices and other sources of data should be imaged and forensically analyzed. If that is not possible, a party may need to move the court for an order requiring preservation, imaging and/or analysis of electronic devices and other sources of data.

Forensic imaging of hard drives is within the scope of discoverable material. *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 652 (D. Minn. 2002). However, the discovery rules are "not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances." Fed. R. Civ. P. 34, advisory committee notes.

Because forensic imaging can quickly become overbroad and intrusive, "Courts have been cautious in requiring the mirror imaging of computers where the request is extremely broad in nature and the connection between the computers and the claims in the lawsuit are unduly vague or unsubstantiated in nature." *Balboa Threadworks*, 2006 WL 763668, at *3. Without a sufficient showing, courts do not allow the "drastic discovery measure" of permitting a party to image an opponent's electronic media. *McCurdy Group v. Am. Biomedical Group, Inc.*, 9 Fed. Appx. 822, 831 (10th Cir. 2001).

Courts are more receptive to circumscribed requests limited to specified individuals or computers expected to produce relevant information.

The Sixth Circuit has observed: "courts must consider the significant interests implicated by forensic imaging before ordering such procedures." *John B. v. Goetz*, 531 F.3d 448, 460 (6th Cir. 2008). Though never granted as a matter of course and difficult to secure, courts are generally more receptive to ordering forensic imaging:

(1) Where the device itself was used to commit the wrong that is the subject of the lawsuit (e.g., the thumb drive that transported the stolen documents; the computer that accessed the trade secrets; etc.); or

(2) If there is evidence that documents were improperly misappropriated, deleted or destroyed.

Following are short case summaries of court cases granting and denying requests for forensic imaging.

a. Examples of Orders Granting Requests for Forensic Imaging

Wagner v. Gallup, Inc., No. 12-cv-1816, 2013 U.S. Dist. LEXIS 191608 (D. Minn. Sept. 18, 2013). After being sued by its former employee, Rodd Wagner, Gallup demanded that Wagner return Gallup's documents. Gallup moved for an order compelling production of Wagner's devices for forensic examination. Magistrate Judge Leung granted Gallup's motion and outlined an 8-part procedure for the forensic examination of Gallup's devices in which a mutually-acceptable computer-forensics vendor would image Wagner's devices and search for Gallup's documents.

M-I L.L.C. v. Stelly, No. H-09-1552, 2011 U.S. Dist. LEXIS 134300 (S.D. Tex. Nov. 21, 2011). The court granted M-I's motion to compel production of forensic images of Stelly's computer because M-I presented reports showing that confidential information was found on USB devices used by Stelly, M-I's former employee. M-I believed that the information was transferred by Stelly to his new firm, WES. The

court concluded that M-I was entitled to discovery in order to determine whether any of its confidential information or trade secrets were uploaded to WES's computers. However, the court determined that allowing M-I full access to the WES's electronic storage devices would unnecessarily jeopardize WES's trade secrets. As a result, the court appointed an independent expert to examine the devices.

Frees, Inc. v. McMillian, No. 05-1979, 2007 U.S. Dist. LEXIS 4343 (W.D. La. Jan. 22, 2007). Plaintiff Frees sought an order to compel its former employee, Defendant McMillian, to produce a laptop and personal computer hard drive, along with other documents. The court granted the motion to compel, but imposed a computer forensics protocol relating to the production of the laptop and computer hard drive. The computer forensics protocol provided six guidelines when producing the laptop and computer hard drive.

Weatherford U.S., L.P. v. Chance Innis & Noble Casing, Inc., No. 4:09-cv-061, 2011 U.S. Dist. LEXIS 59036 (D. N.D. June 2, 2011). Plaintiff Weatherford sued its former employee, Innis, and his newly formed company, Noble Casing, Inc., claiming that Innis downloaded a number of files from Weatherford's intranet site onto a thumb drive and that Innis used those documents to "jump start" Noble Casing. Innis claimed he did not later access the downloaded files. But a forensic expert reported that the files were accessed on numerous occasions. Weatherford moved to compel access to all computers owned by Noble Casings and used by its employees since its inception as well as any and all portable storage devices that had been plugged into these computers. Weatherford supported its broad request based on the discrepancy between Innis's deposition testimony and the findings of its forensic expert. The court found that Innis's acknowledgment that he downloaded Weatherford files to a thumb drive without permission was itself enough to provide a nexus between Weatherford's claims and its need for images of the computers. Thus, the court granted Weatherford's motion to compel and ordered a five-part imaging, recovery and disclosure process.

Lifetouch Nat'l Sch. Studios, Inc. v. Moss-Williams, No. C10-05297, 2013 U.S. Dist. LEXIS 148360 (N.D. Cal. Oct. 15, 2013). Plaintiff Lifetouch sought computer forensic imaging after a former employee, Defendant Moss-Williams, copied her hard drive at Lifetouch onto a thumb drive and viewed the contents of the thumb drive on the laptop of her new employer, Defendant Creative. Moss-Williams proceeded to destroy the thumb drive after determining she did not need the information. Lifetouch argued that due to Moss-Williams' destruction of the thumb drive, its only recourse was to examine Creative's computers that Moss-Williams may have used to view the contents of the thumb drive. The court determined that there was a sufficient nexus between Creative's computers and the alleged misappropriation of trade secrets to warrant forensic imaging of the computers.

AutoNation, Inc. v. Hatfield, No. 05-02037, 2006 WL 60547 (Fla. Cir. Ct. Jan. 4, 2006). In order to prevent Plaintiff AutoNation from suffering immediate and irreparable harm from misappropriation of trade secrets by Defendant Hatfield, the court granted temporary injunctive relief. The court ordered Hatfield to return all

copies of information containing any information concerning AutoNation. Additionally, the court ordered a laptop be made available to AutoNation for examination by a forensic computer expert in order to determine whether certain emails Hatfield sent had been forwarded or otherwise altered or used. The court authorized Hatfield to have an independent forensic expert available and in attendance at the inspection.

United Factory Furniture Corp. v. Alterwitz, No. 2:12-cv-00059-KJD-VCF, 2012 WL 1155741 (D. Nev. Apr. 5, 2012). Plaintiff United Factory Furniture ("UFF") filed Motions for Order to Preserve Evidence, Preliminary Injunction, and a Mirror-Imaging Order. UFF alleged the defendants created a secret access to the company server and accessed confidential information. The court denied the motion for preliminary injunction and a preservation order, but granted the mirror-imaging order. The court used a five-point analysis in weighing the benefit and the burden of the discovery. The mirror-imaging order was found to be appropriate "to maintain the status quo." The court specified a protocol for the mirror-imaging, including the appointment of an agreed-upon forensics expert.

b. Examples of Orders Denying Requests for Forensic Imaging

Pure-Flo MPC, LLC v. Bio Fab Techs., Inc., No. 06-C-505, 2006 U.S. Dist. LEXIS 35116 (E.D. Wis. May 12, 2006). Plaintiff Pure-Flo moved for expedited discovery and also requested permission for immediate inspection and copying of the complete contents of each computer that the defendants used to access, receive, copy, or use data or documents that were transmitted or copied from a Pure-Flo computer or network. The court denied the motion for expedited discovery because Pure-Flor had not yet filed a motion for a preliminary injunction.

Balfour Beatty Rail, Inc. v. Vaccarello, No. 3:06-cv-551-J-20MCR, 2007 WL 169628 (M.D. Fla Jan. 18, 2007). Plaintiff Balfour Beatty Rail ("BBR") alleged that Defendants Vaccarello and Byers, its former employees, conspired and undertook to damage its computers and destroy information on the computer in order to set up a competing enterprise, ARS Corporation. BBR moved to compel discovery regarding computer hard drives used by Vaccarello or Byers for ARS or BBR business purposes. The court denied BBR's request because BBR did not provide any information regarding what it sought to discover from the hard drives. Further, BBR did not make any contention that Vaccarello and Byers failed to provide the requested information contained on the hard drives. Because BBR made no showing that justified access to the hard drives, the court found that BBR's request would permit an unauthorized fishing expedition.

Fasteners for Retail, Inc. v. DeJohn, et al., No. 100333, 2014 WL 1669132 (Ohio Ct. App. Apr. 24, 2014). Plaintiff Fasteners for Retail ("FFR") filed suit against Defendant K International ("KI"), alleging misappropriation of trade secrets and patent infringement, among other claims. During the course of litigation, FFR learned that Defendants DeJohn and Kump, former employees of FFR, performed consulting work for KI. FFR filed suit against DeJohn and Kump, alleging that DeJohn and

Kump breached the confidentiality and nondisclosure provisions of their employment agreements, misappropriated trade secrets, and engaged in unfair competition. FFR moved to compel DeJohn and Kump to provide their computer hard drives for forensic imaging, which the trial court granted. Defendants appealed the trial court's order. The Ohio Court of Appeals reversed and concluded that the record did not demonstrate the requisite showing of defendants' noncompliance with discovery and the trial court's order did not contain a protective protocol. The appellate court therefore determined that the trial court abused its discretion by ordering forensic imaging of the computer hard drives.

VII. CONSIDERATIONS IN SEEKING FORENSIC IMAGING AND ANALYSIS FROM A COURT

In the context of a non-compete or trade-secret case, when a plaintiff has strong evidence that a former employee or other individual stole confidential information or trade secrets, it should consider taking immediate steps to secure the devices at issue and image them.

If the opposing party is unwilling to make available the relevant images, the plaintiff should consider filing a motion with the court (either accompanying or after a motion for a TRO or preliminary injunction is filed). It generally is not a good idea to file such a motion before emergency injunctions are filed. *See, e.g., Pure-Flo MPC, LLC v. Bio Fab Techs., Inc.*, 2006 WL 1389115 (E.D. Wis. May 12, 2006) (denying request for forensic imaging where plaintiff had not yet filed its preliminary injunction motion: "The Court will not accelerate and expand discovery beyond the parameters annunciated in the Federal Rules of Civil Procedure so as to help the parties prepare for an evidentiary hearing that may never take place.").

When seeking forensic imaging along with a TRO or preliminary injunction, a plaintiff generally may want to:

- ✓ Submit a record of having made an **informal request** to the defendant for images of the devices at issue.
- ✓ Submit a draft **forensic protocol** that takes adequate steps to protect the privacy of defendant's devices and any privileged communications.
- ✓ Ask the court for an order requiring the defendant to **preserve** and not delete all relevant and discoverable information (and give examples of that type of information).
- ✓ Submit an **initial report** from a forensic expert or consultant outlining the problematic behavior that has occurred to date in order to justify the request for a forensic imaging (and pique the court's interest).
- ✓ Have a reasonable proposal about **who pays** for the imaging.

a. Requesting Forensics – Informally and Formally

Unless emergency ex parte relief is necessary, most judges want to see parties attempt to resolve disputes before filing a motion and many courts require parties to meet and confer before filing a motion. As a result, parties should consider requesting the opposing party to voluntarily allow for forensic imaging of the relevant devices subject to protocols to protect privileged and private information (see the next subsection on forensic protocols).

b. Forensic protocols

When courts grant access to a device, they almost always establish or approve a protocol to protect the party's privacy and any privileged information. *See, e.g., Fasteners for Retail*, 2014 Ohio App. LEXIS 1684, at *18 (court must (1) determine if imaging is justified in light of privacy concerns and (2) enter a protective protocol governing the imaging).

If a party is unable to convince an opposing party to voluntarily allow for forensic imaging of the devices and a formal motion is necessary, that party should include a draft protocol for imaging and analyzing the devices with its motion. At a minimum, the protocol should address what devices will be imaged and analyzed; how they will be imaged and analyzed; who will have access to the images; how privileged information will be protected; how private information will be protected; and how responsive and relevant documents and metadata will be produced. An example of a relatively straightforward annotated protocol is attached as Exhibit A to this paper.

c. Preservation orders

When seeking the forensic imaging and analysis of devices, the moving party may also want to ask the court to order that all devices containing the former employer's confidential information or trade secrets be preserved. Though parties already are required to preserve relevant information and not destroy evidence, preservation orders bolster that requirement and provide additional protection to the former employer. In addition, if the devices are in continuous use, there is the possibility that data could be overwritten or deleted through normal usage of the device. *See Antioch*, 210 F.R.D. at 651-52 (ordering imaging of computers where defendants "may have relevant information...which is being lost through normal use of the computer").

d. Initial expert reports

When moving to compel forensic imaging and analysis, it is good practice to give the court justification for why such imaging is necessary. This can often be done through the initial report of a computer forensics expert. Though only a certain amount of data may be available, the expert can inform the court of any suspicious activity and evidence of misappropriate of trade secrets. *See infra* Section VIII on expert affidavits.

e. Who Pays?

The party requesting the forensic imaging and analysis typically offers to pay for it—at least at the initial stage—in order to secure the data as quickly and efficiently as possible. That said, there may be circumstances when it is appropriate for the moving party to ask the owner of the devices to pay for the imaging—especially if there is clear evidence of wrongdoing. Regardless, the party moving for forensic imaging and analysis, should make a reasonable proposal regarding who will cover the fees and costs.

VIII. EXPERT AFFIDAVITS

In order to secure a TRO, preliminary injunction, or an order for more thorough forensic imaging, it may be advantageous to submit an affidavit from a forensic expert or consultant.

An affidavit of a forensic expert or consultant should provide the court what it needs to rule in favor of your client. Such reports may include:

- The expert's qualifications and CV, including his/her background, practical experience, and other cases where he/she has submitted a report or testified.
- The expert's compensation. If true, make clear that the expert does not receive money based on the outcome of the litigation.
- Some background on computer forensics procedures and how it is determined whether data has been copied, transferred, deleted, altered or otherwise used.
- Describe key forensic concepts such as "active files," "unallocated space," and "link files."
- Describe platforms where data was stored. For example, if the defendant used Dropbox to misappropriate trade secrets, the expert should explain what Dropbox is and how it works.
- Describe the initial evidence recovered from the defendant's computers and devices.
- Explain why a full forensic image of computers and other devices would be beneficial to the case and to the court.

In addition, we recommend including visuals or demonstratives—either within the affidavit itself or as an exhibit to the affidavit. Show the court—visually—how data was transferred; how much data was transferred; or photos of the devices used to steal the trade secrets.

IX. PRESENTING COMPUTER FORENSICS AND TRADE SECRET THEFT TO JUDGE OR JURY

Computer forensics is a complicated field and not all judges and jurors will have the same level of experience with technology. For this reason, we recommend keeping any presentation of forensic evidence simple, easy to follow, and digestible. We also recommend using visuals to tell a compelling story.

a. KISS – Keep It Simple

Expert affidavits may need to include a lot of technical jargon to educate the court. Such affidavits should be presented in clear and straightforward language.

But when explaining how data transferred from one device to another, it is important to simplify the message. Avoid using technical jargon and, if you do, explain it.

b. Use Visuals

Visuals and demonstrative exhibits can be extremely compelling when presenting digital forensics in a non-compete or trade-secret case. Examples include:

- ✓ Timelines contrasting key dates (for example, comparing (1) the employee's resignation date, last day of employment at former employer, and first day of employment at new employer with (2) the dates when the former employer's confidential information or trade secrets was accessed or transferred).
- ✓ Flow charts showing the journey of data from one device to another (for example, from the former employer's computer to a Dropbox account to a USB device to the new employer's computer).
- ✓ An illustration showing how the former employer's trade secrets were used and disseminated to a broader audience.
- ✓ Etc.

X. WORKING WITH FORENSIC EXPERTS

a. Selecting the right expert for the right case

As with all experts, it is important to find the right "fit." Is the expert able to simplify and effectively explain complicated concepts? Will the expert be able to explain these concepts to a judge or jury? Is he or she responsive and does he or she prioritize your case?

Preservation and routine report processing is typically performed by a junior examiner. For cases involving expert witnesses, it is helpful to have subspecialties (e.g. reverse engineering of malware, Mac forensics, database analysis) in addition to prior testimonial experience. Care should be given to ensure the expert is close to the hands-on experience in the case.

b. Privilege considerations

Consider that some communications between counsel and forensic expert or consultant might not be protected from disclosure. An in-depth discussion of what is and is not protected is beyond the scope of this paper. In general, however, a non-testifying expert's work will likely be considered protected from disclosure by the work-product doctrine. With respect to testifying experts, rules among the various state courts differ. In federal court, however, experts' draft reports are protected by the work-product doctrine. Fed. R. Civ. P. 26(b)(4)(B) expressly provides that the doctrine applies to "protect drafts of any report or disclosure required under Rule 26(a)(2), regardless of the form in which the draft is recorded." The Federal Rules also protect communications between experts and the counsel who retain them, except (1) communications pertaining to the expert's compensation, (2) facts or data that the attorney provided and the expert considered in forming opinions, and (3) assumptions that the attorney provided and that the expert relied on. Fed. R. Civ. P. 26(b)(4)(C).

c. Fee arrangements

Digital forensics are usually charged on an hourly basis or a project cost based on the number of devices. Examiners on average cost about $325 per hour between a range from $275 per hour to $750 per hour depending on specialty and geography. Storage costs, online storage costs and other fees should be explored to ensure one is comparing "apples to apples" in costs. Imaging a device has numerous factors in cost depending on the size of the device. It typically costs anywhere from $300-$1000 to preserve and image a device. Additional costs are incurred for forensic processing and analysis (e.g. recover folders, Internet history, removable device activity).

d. Types of forensic analysis

i. Imaging

Forensic imaging involves using generally acceptable tools and techniques to preserve data usually by creating a "bit for bit" copy of a hard drive with a hash value serving as a digital fingerprint. Numerous copies can be made of the original image into "working copies" and forensic software can compute the matching hash to determine that no alteration of the data has occurred. A write blocker is usually used during this process so the examiner does not "stomp" on the metadata of the pertinent files.

ii. Triage or "quick and dirty" analysis

The purpose of triaging or a "quick and dirty" analysis is to look for key indicators of trade secret theft to determine if further analysis is necessary. Such an analysis of a device can be conducted by software on live systems or even from a preserved network share or hard drive. The more experienced the examiner the easier this technique becomes to drill down to the substantive data. The main area to look at in a Windows system is the <USER> or custodian directory that contains the desktop, My Documents, downloads, web browser files and the <USER> registry file NTUSER which can identify removable device information (there are different Registry files we may also look at from the SYSTEM* directories).

iii. Targeted analysis

Targeted analysis is often used as part of Subsection ii above with numerous systems or with the use of an agreed or ordered protocol involving certain types of files (e.g. .DOC, .DOCX for Word documents), a specified date range or other agreed upon parameter. This can also be used by using keyword searches and/or avoiding certain privileged or confidential material.

iv. Full-fledged analysis

A complete analysis is conducted by forensically processing the data/hard drive and using certain tools and techniques to recover and comb through the data. Active and deleted files are identified in spreadsheets; data integrity/wiping artifacts are examined to determine if they are present; and both user and system logs, caches, activity and behavior are reviewed. A few examples of this are:

- Keyword searching of allocated and unallocated space (including search for possible deleted and partially overwritten sectors on a disk).

- Using a reporting tool like Magnet Forensics' Internet Evidence Finder (IEF) to carve out web browsing history, Google searches, USB usage, link file (.LNK) analysis, etc.

- Identifying "unsearchable" documents that may need human inspection or a post-processing tool to convert a proprietary format (e.g. Outlook PST/OST files, scanned images, certain PDF documents).

- Review Windows Event logs (PLISTs, SQLite database in Mac OSX), REGISTRY keys and program logs for activity. For example, if the examiner sees a program like CCLEANER, he or she will look for wiping activity. Moreover in the file system CCLEANER often makes an extension in the form of .ZZZ which would become apparent as the examiner reviews the file spreadsheets.

- Timeline file metadata, program activity and user activity using the file spreadsheets; Most Recently Used lists from files; and program REGISTRY values and correlate with browser/email/USB activity.

The list can get very long, so communication and understanding between counsel and examiner is very important to focus any examination and control time and costs.

These materials are for educational purposes only and do not represent the views of the authors or any of their clients.

EXHIBIT A

Disclaimer:

This is a sample form provided only for educational purposes and has not been approved by a court or Minnesota CLE. This form should be tailored to meet the specific requirements of your unique case and any other legal requirements particular to the jurisdiction in which your case is venued.

Oldco, Inc. vs. Former Employee
SAMPLE FORENSIC PROTOCOL

This Forensic Protocol ("Protocol") sets forth the timing and procedure for the inspection of the _____ ("Devices") in the possession, custody or control of Former Employee ("Former Employee"), as well as the Yahoo! Account Former Employee created, stolendocs@yahoo.com ("Yahoo! Account"). Former Employee has represented that the Devices are the only electronic devices in his possession that are capable of storing or creating Oldco documents. If it is discovered that other electronic devices or media contain Oldco documents, Former Employee agrees to make those devices and/or media, as well as any necessary credentials, available for inspection and that this Protocol also applies to the inspection of those devices.

A. Delivery of Devices and Imaging.

1. On or before Monday, May 29, 2017, or as soon thereafter as practicable, Forensic Expert shall travel to Former Employee's home and create a forensic image(s) of the Devices (the "Forensic Images") and perform an analysis in accordance with the provisions of this Protocol. Forensic Expert will not remove the Devices from Former Employee's home and Former Employee may be present to observe the imaging process.

2. Neither the parties nor their counsel may at any time view the Forensic Images. Rather, access to the Forensic Images is limited to Forensic Expert, and any qualified expert retained by Former Employee. If Former Employee chooses to retain an expert to conduct an analysis of the Forensic Images, Forensic Expert shall, upon request, promptly provide Former Employee's expert with a copy of the Forensic Images at no additional charge to Former Employee, other than the cost of any required storage media used to transfer the Forensic Images.

B. Restrictions and Analysis of Devices.

1. The parties agree that the Forensic Images created by Forensic Expert pursuant to the terms of this Protocol will be used solely in

connection with *Oldco, Inc. v. Former Employee,* which is currently pending before the Hennepin County, Minnesota District Court (the "Litigation"), and not for any other purpose or function.

2. The parties agree that the creation of Forensic Images pursuant to this Protocol is intended to permit Forensic Expert and any expert retained by Former Employee to conduct a forensic analysis of the Devices, without permitting counsel to have direct access to the contents of the Devices.

3. Upon creation of the Forensic Images, Forensic Expert may analyze such images for the purpose of determining whether Former Employee retained, opened or otherwise accessed, copied or transferred, or deleted any Oldco documents, including but not limited to those e-mails (and attachments) that Former Employee forwarded to the Yahoo! Account. Forensic Expert may disclose to Oldco's counsel its opinion whether Former Employee engaged in any of these activities and the underlying basis as to how it arrived at those opinions. Forensic Expert also may produce to the parties' counsel copies of any Oldco documents that Former Employee retained, opened or otherwise accessed, copied or transferred, or deleted. Forensic Expert may not disclose to Oldco and its counsel the contents of any communications between Former Employee and his counsel. To that end, Forensic Expert will first provide copies of any documents believed to be Oldco documents only to Former Employee's counsel, and allow 48 hours for review of the documents to determine if they are privileged communications or protected trial preparation materials. If Former Employee's counsel assert any objection on the grounds of privilege or work product, Forensic Expert may not provide the documents to Oldco's counsel until the objections have been resolved by agreement or *in camera* review by the Court. Former Employee may, at his option, retain his own expert to conduct a separate analysis of the Forensic Images. Nothing in this paragraph or in the Protocol in general shall be deemed an admission by any Party to this Protocol that any particular document is (or is not) an "Oldco document." Further, the Parties agree that they wish to preserve any and all arguments related to any document or communication identified by this Protocol including, but not limited to, those related to the discoverability, relevancy, or admissibility of any document or communication identified pursuant to this Protocol.

4. If it is discovered that Oldco documents remained on Former Employee's Devices following the termination of his employment with Oldco, the parties agree to coordinate in good faith and Former Employee agrees to make the Devices available in order to permanently delete those documents from the Devices in a forensically-sound manner.

5. Upon the conclusion of the Litigation, Oldco shall direct Forensic Expert to destroy the Forensic Images and Oldco shall provide a statement to Former Employee's counsel when such destruction is complete.

6. Forensic Expert also shall be given custody and control of the Yahoo! Account and shall: (1) create a new password to prevent further access to the account by Former Employee or his counsel, which will not be shared with Oldco or Oldco's counsel; (2) if appropriate, create a forensic copy of the Yahoo! Account; and (3) conduct a non-destructive review of the account to determine (a) whether it has been accessed by Former Employee; (b) whether any other Oldco e-mails other than those produced by counsel for Former Employee were forwarded to this account; and (c) whether any e-mails were sent or forwarded from this account. Forensic Expert shall report its findings to counsel for both parties, and provide copies of any documents or data that support its findings, subject to the proviso in Paragraph 3 above regarding review by Former Employee's counsel prior to disclosure of any documents to Oldco. Former Employee may, at his option, retain a qualified expert to perform a separate analysis of the Yahoo! Account, in which case the account password will be provided to the expert so designated. Upon the conclusion of the Litigation, Oldco shall direct Forensic Expert to destroy the contents of the Yahoo! Account.

7. Oldco will pay Forensic Expert's fees and costs that are associated with preparing and analyzing the Forensic Images. However, this provision will not be deemed a waiver of Oldco's right to pursue recoverable costs.

PLAINTIFF'S LAW FIRM
As counsel for Plaintiff Oldco, Inc.

By: _____ Dated: _____, 2017

DEFENDANT'S LAW FIRM
As counsel for Defendant Former Employee and Defendant Newco, Inc.

By: _____ Dated: _____, 2017