CIA Computer
Investigative
Associates

May 4, 2010 **<u>Prepared for Counsel</u>**

Peter A. Biagetti, Esq.
Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.
One Financial Center
Boston, MA 02111

Re: Cetin Dogan Matter

Dear Peter:

Computer Investigative Associates has been asked to review the accuracy of data allegedly stored on certain CDs, DVDs, and electronic files to which our clients have been denied access. We look forward to undertaking a more definitive analysis as soon as our clients are granted that access, but in the meantime, we can confirm that:

(1) It is very easy for the user of a computer to alter many pieces of information stored on that computer, including the purported date or author of a document stored on that computer, or the purported IP address of that computer.

(2) Windows™ systems do not generally mark documents or files with information that easily allows for the accurate identification of their origin.

(3) As a result, any document or file must be examined in the context of the whole system from which it originated before anyone may be certain of its accuracy or completeness. Because no such examination has been done here, *the documents and files at issue may be totally inaccurate as to date or time created, author, company, system origin and/or constituent information.*

More specifically, we were asked to research and reply to questions regarding the data stored in CDs, DVDs, and computer systems, as well as the nature and accuracy of data stored in certain Microsoft Office™ files (also referred to as the meta-data). Again, however, *we have not been given access to the original documents or data storage media*, so our analysis to date has been limited to the general nature of data storage, accuracy of specific data, and the nature of Microsoft Office™ documents and the limitations of analyzing date timestamps without access to the system itself. It is therefore essential to emphasize that many of the pieces of identifying information in computer files and on computer systems are "user selectable," meaning that *a user of the system can change any of that information at any time*. The computer system itself generally does nothing to ensure that identifying data is accurate or true.

Date and Time: It is always possible that either the date or time set on a computer is inaccurate or that the date or time on a particular file is inaccurate. Computers by their nature rely on the user to set the date and time. When the system starts up, it is quite simple for the user to go into the BIOS (Basic Input Output System) and set the date or time to whatever the user wants. Any files created or accessed from that point on will reflect the changed date or time. This also happens when the internal battery on an older computer system is drained -- the internal clock loses it accuracy and, once the battery is dead, the system likely will ask the user for a new date and time upon startup, or merely use some arbitrary date or time determined by the manufacturer. There are technical ways of dealing with these possible distortions -- such as locking the BIOS or forcing the system to get its date or time from a time server -- but we have seen no evidence presented that such safeguards were taken in this case.

Of course, any file created on a computer once the date or time has been changed will reflect the altered date or time. This would include Microsoft Office™ documents created on that computer, documents scanned into the computer, or emails from the computer (though in the case of emails, since there is a server processing the email, the time may well be adjusted to reflect the time as the server knows it). Similarly, any CDs or DVDs created on the system would reflect the altered date or time. As a result, to conduct a definitive investigation of the accuracy of date and time information, one must thoroughly examine, for example, the system log files to determine if there were entries that did not appropriately match the timeframe in which the computer was in use, as well as other contextual information that may support the date pattern on whatever documents/files are in question. *Absent the original computer system and appropriate forensic investigation of the system, there simply is no way to responsibly determine the date or time of any file purportedly created on a particular system.*

Author: The meta-data retained by documents created using Microsoft Office™ does include information recording the purported "author" of the document, but *this information reflects only the computer used, not the person who may have used that computer to create the document*. As with dates and times, this "author" data can easily be changed by the user, either when the document is created or anytime after that, simply by right-clicking on the document, selecting "Properties," going to the "Summary" tab, and changing the "author's" name. This same, simple process may also be used to change any "Company" information stored in the meta-data.

Origin: As explained above, while many documents and certain files contain easily altered information regarding their purported "Author" or "Company," *most do not record in any way the specific computer system from which they originated.* While there may be some exceptions, such as media files (usually containing music or movies) in which Digital Rights Management (DRM) software or hardware is employed, virtually *no* software used to create CDs or DVDs employs these DRM controls when creating disks that contain files or documents *not* designed for media playback. As a result, linking a CD or DVD to a specific computer system is generally done by examining all of the properties of the documents on that CD or DVD, as discussed above, while staying mindful that many of those properties can be altered by a user.

IP Address: Finally, *even the IP addresses noted within files on a computer may be altered by the user*. Generally, files and documents do *not* retain IP-address information about the system on which they were created. Certain work-sharing software (such as Lotus Notes™ or Microsoft Exchange™) may provide this information as part of the workflow process, but they also allow it to be set by the user. As a result, no responsible examiner could ever accept the IP address from any particular file without reviewing all corroborating network information (log files, network traffic captures, etc). It is just too easy for someone to change the IP address on a system to create a file that reflects a desired address rather than the address of the system which in truth created the file.

Conclusion: It is the opinion of Computer Investigative Associates, that absent an examination of the originating (or purportedly originating) system by a qualified forensic analyst, the accuracy of meta-data in documents or the date time stamps on any computer file is suspect and can not responsibly be seen as fact.

Sincerely,

John D. Tessel, CISSP

CTO
Computer Investigative Associates, LLC