

**CHEVRON CORP AND TEXACO PETROLEUM COMPANY
V.
THE REPUBLIC OF ECUADOR**

EXPERT REBUTTAL REPORT OF J. CHRISTOPHER RACICH

DECEMBER 16, 2013

I. BACKGROUND AND QUALIFICATIONS

1. Vestigant, LLC ('Vestigant') was retained by Winston & Strawn, LLP ('Winston') to review the reports written by Mr. Spencer Lynch with regards to the above captioned matter, and identify and rebut various statements that are inaccurate or misleading in these reports.

2. I am the President of Vestigant. Vestigant is a technology and computer forensic consulting firm that assists clients with fact-finding in litigation, regulatory reviews, and business decisions. I founded Vestigant in 2009 and since that time Vestigant has been retained in hundreds of Computer Forensic and E-Discovery cases.

3. I am a 1993 graduate of Cornell University where I received my Bachelor of Arts degree (Biology). I later attended law school at the Washington College of Law at American University, graduating with a Juris Doctor in 1997.

4. I have taken numerous courses and attended multiple seminars in the field of computer forensics over the past 16 years. I have taught computer forensics courses at the High Technology Crime Investigation Association (HTCIA). I am also an adjunct Professor of Law at the Washington College of Law at American University where I teach a course concerning electronic discovery.

5. During my career in the computer forensics field, I have provided testimony as an expert in computer forensics in numerous courts, including the United States District Court for the Eastern District of Virginia, the United States District Court for the Southern District of Florida, the United States District Court for the Southern District of Texas, the Superior Court for the District of Columbia, the Missouri Circuit

Court, the Supreme Court of the State of New York, County of New York, the Larimer County District Court in Colorado, and the Pennsylvania Court of Common Pleas. I have also provided expert deposition testimony in the area of computer forensics in connection with numerous civil claims, and have also testified as an expert witness before the National Labor Relations Board. I have been qualified at least 22 times as an expert in computer forensics in a court of law or arbitration proceeding.

6. A copy of my curriculum vitae is attached to this Report as Exhibit A. It (a) describes my education, employment, and qualifications, (b) summarizes my experience in the area of computer science and computer forensics, and (c) lists the cases in which I was qualified as an expert in computer forensics, and the publications that I have authored in the last 10 years.

II. COMPENSATION

7. Vestigant is being compensated by the client in this case at an hourly rate of between \$325 and \$500 for my work on this engagement, depending on the nature of the tasks performed. My compensation is not affected by the outcome of this case or the contents of this report. Various research and support tasks related to this engagement have been performed for me by others employed at Vestigant under my direction.

III. MATERIALS CONSIDERED

8. In preparation for rendering this report, I reviewed and analyzed the following materials:

(a) The Expert Report of Spencer Lynch dated October 7, 2013 and Exhibits, in the above captioned case (Lynch October Report).

(b) The Expert Report of Michael L. Younger dated January 24, 2013 and Exhibits, in the above captioned case (Younger January Report).

(c) The Supplemental Expert Report of Michael L. Younger dated February 28, 2013 and Exhibits, in the above captioned case (Younger February Report)

(d) The Supplemental Expert Report of Michael L. Younger dated May 31, 2013 and Exhibits, in the above captioned case (Younger May Report).

(e) One hard drive that contained what has been identified to be forensic images of computers and media reviewed by Mr. Lynch. A full list of the image names included on this hard drive is attached as Exhibit B.¹

IV. SCOPE OF ANALYSIS

9. On August 27, 2013, I received from Winston & Strawn a hard drive containing forensic images of a hard drive and other media reviewed by Mr. Younger and Mr. Lynch in support of their reports. I was asked to analyze the media based upon the opinions that Mr. Younger and Mr. Lynch provided in their expert reports. It is my understanding that Mr. Lynch's report has now superseded Mr. Younger's earlier reports and consequently I will respond below directly only to Mr. Lynch's report.

10. I reserve the right to supplement my report or opinions should additional information become known to me.

¹ I am only able to authenticate the images I reviewed with regards to their being the same images that have been reviewed by Mr. Lynch. I have no independent Chain of Custody documentation that shows that the media that these images were created from were in possession of former Judge Guerra.

V. SUMMARY OF CONCLUSIONS

11. There is a lack of information with regards to the chain of custody of the media analyzed by Mr. Lynch. Based upon provided documentation, it appears that after Mr. Guerra released the media to Andres Rivero over 22,000 files and folders on the Guerra hard drive had their Last Access Dates updated, indicating that these files had been touched or manipulated in some way.² There also appears to be a two day gap after the media was released to Andres Rivero and when the imaging occurred, during which time, data manipulation could have occurred.

12. In the Lynch October Report, Mr. Lynch's 'Authentication' of the documents from former Judge Guerra's media shows only that the documents were on the analyzed media as of the moment the forensic images were made on July 15, 2012. This does not authenticate the documents as to their origin, author, or editor.

13. In the Lynch October Report, Mr. Lynch identifies 11 documents on the provided images that have textual similarities to orders issued by Judge Zambrano in the Lago Agrio Litigation. Mr. Lynch assumes that these were all documents written by former Judge Guerra but the forensic analysis does not authenticate that these documents were in fact created by, authored by, or edited by former Judge Guerra. In fact, the metadata shows only that the documents existed in another location and were copied to the former Judge Guerra's media *after* they were last modified.

14. In the Lynch October Report, Mr. Lynch identifies 105 documents on the provided images that have textual similarities to orders issued by the Lago Agrio court in cases *other than* the Lago Agrio Litigation. Mr. Lynch again assumes that these

² This access occurred on or after 2:53 pm on July 13, 2012.

were all written by former Judge Guerra. Indeed, the metadata indicates only that each of these files appear to have been created from a template created on a computer that was not reviewed or obtained by Lynch. This is indicated by the identical internal Created Dates of the documents, the identical last Print Dates of the documents and the Author information in each of the documents. However, just because the documents appear to be created from a ‘template’ document does not mean that former Judge Guerra was involved in the creation or modification of the content of these documents. Mr. Lynch provides no forensic evidence to show this.

15. In the Lynch October Report, Mr. Lynch describes the process he used to identify the textual similarities between the documents found on the analyzed media and documents in the Ecuador Court filing systems. While this process appears to be technical in nature, this does not rely on any forensic expertise and provides no information about the origin of these documents found on Guerra’s media. Nothing in my review of the Beyond Compare software indicates that one needs any special forensic or technical skill to run or operate this software.

VI. ANALYSIS

16. Mr. Lynch states in section 2.1 of the Lynch October Report that Gibson Dunn asked Stroz Friedberg to perform the following tasks, among others:

- (a) Authenticate and analyze forensic images of a computer and various storage devices belonging to former Ecuadorian Judge Alberto Guerra and compare 11 extracted documents to determine their chronological relationships, to identify their similarities with one another, and to analyze the metadata associated with each;

- (b) Authenticate and analyze the 11 extracted documents from former Judge Guerra's media and compare them to nine orders issued by former Ecuadorian Judge Nicolas Zambrano in the Lago Agrio litigation;
- (c) Authenticate and analyze 105 extracted documents from former Judge Guerra's media and compare them to rulings issued in other matters in the Ecuadorian Court System;
- (d) Authenticate and extract data from two Nokia cell phones belonging to former Judge Guerra;
- (e) Authenticate and extract data from an email account belonging to former Judge Guerra.

17. I have focused on specific areas of Mr. Lynch's forensic analysis concerning former Judge Guerra.

A. CHAIN OF CUSTODY OF GUERRA MEDIA

18. While Mr. Lynch describes the Chain of Custody of the images that Stroz Friedberg received once they were in the possession of Stroz Friedberg employees, there are significant questions about the Chain of Custody of the media prior to Stroz Friedberg receiving the images.

19. In the forensic industry, it is a standard part of the forensic process to maintain a good Chain of Custody for media that is being examined. A Chain of Custody is a document that is transferred with evidence that identifies who had custody of the media/images, when they received custody of the media/images, and to some extent, what alterations could have taken place on the media/images.

20. A forensic examiner can only authenticate media and data within the bounds of the Chain of Custody that they possess. In this case, no Chain of Custody documentation has been provided that demonstrates that the images that Mr. Lynch reviewed were in fact of devices owned by former Judge Guerra or documenting any

alterations made to the devices after they were received but before they were forensically imaged. This lack of Chain of Custody should at least be addressed with regards to the authentication of the data on the media.

21. Based upon the materials I have reviewed, there also appears to be a two-day gap between when the media was purportedly seized on July 13, 2012 from former Judge Guerra and when the media was imaged on July 15, 2012.³ There is no way to identify what activity took place on the media during that two-day gap.

22. If one relies on the testimony of Andres Rivero, it appears that the media was seized from former Judge Guerra in the morning of July 13, 2012. However, over 22,000 files and folders on the media had their Last Access Date updated in the afternoon and evening of July 13, 2012, a fact not addressed by Mr. Lynch or the chain of custody documentation. Nor does Mr. Lynch or the chain of custody documentation address the fact that activity may have taken place on the media seized from former Judge Guerra between July 13, 2012 and July 15, 2012 when the media was imaged.

B. MR. LYNCH'S ATTEMPTED AUTHENTICATION OF THE 11 DOCUMENT SET

23. In the Lynch October Report, Mr. Lynch attempts to authenticate a set of 11 documents found on Guerra's hard drive that Gibson Dunn requested he review.

24. Mr. Lynch compares the 11 documents to nine orders issued in the Lago Agrio Litigation and claims that it is apparent the nine issued orders were created from the drafts located on the Guerra hard drive.⁴ Based on the available forensic evidence, Mr. Lynch's conclusion is unsupported. Nothing in the provided forensic analysis

³ Deposition transcript of Andres Rivero

⁴ Lynch Expert Rpt. ¶ 28.

indicates that the issued orders were created from the drafts found on Guerra's computer or that Guerra himself was the author of any of these orders.

25. Mr. Lynch goes into some detail regarding the comparison of what he identifies as 11 Draft Guerra Orders to orders issued by Judge Zambrano in the Lago Agrio Litigation. This analysis includes (1) comparison of the acquisition hash values of the electronic media to the hash values of the images in Mr. Lynch's possession, (2) textual comparison of the 11 documents to actual documents issued by Judge Nicolas Zambrano, and (3) review of the "Last Modified" date of the 11 documents in comparison of when the documents issued by Judge Nicolas Zambrano were filed. While Mr. Lynch's analysis of the 11 documents appears technically correct, nothing in his analysis leads to his conclusion that the orders issued by Judge Zambrano were created from the drafts located on the Guerra hard drive.⁵

26. **First**, it is true that the acquisition hash value of the Guerra hard drive image matches the current hash value of the EnCase image file of the Guerra hard drive. However, that does not authenticate the documents that exist on the media. It means only that no changes have been made to the forensic image since the imaging was done, in this case on July 15, 2012. This level of authentication authenticates only the image itself, not any of the content found within the image.

27. **Second**, Mr. Lynch describes the process he uses to compare the textual content of certain documents to orders found in the Ecuadorian court system. While Mr. Lynch's process does in fact do a comparison of these documents, the comparison of these documents is not an application of forensic science.

⁵ See Lynch Expert Rpt. ¶¶ 2(c), 28.

28. While technological in nature, the comparison done by Mr. Lynch is akin to simply reading two documents and identifying similarities and differences between these documents. This process does not require any forensic ability to perform.

29. Review of Mr. Lynch's analysis of the textual content of the 11 total documents in comparison to the Ecuador filings using off the shelf software appears to be relatively accurate with regards to the similarities between the documents. However, nothing in the performed analysis indicates that the 11 documents were in fact drafts authored by former Judge Guerra.

30. **Third**, Mr. Lynch implies that due to the fact that the documents he reviewed were modified shortly before the Lago Agrio Litigation orders were issued that this means that these 11 documents were the drafts of the actual orders in the Lago Agrio Litigation.⁶ He also states that “[b]ased on the comparisons described above it is apparent that the nine issued orders were created from the drafts located on the Guerra hard drive.”⁷ This is not the case. The comparison shows only that these documents have similar textual content and that they were last written on their Last Saved Date. There is no forensic evidence provided that indicates that former Judge Guerra was the author of these documents, or made any changes to these documents, or that they were ever provided to Judge Zambrano.

31. Significantly, all 11 of the documents reviewed by Mr. Lynch were created on the Guerra Hard Drive on July 23, 2010, the same day the operating system was installed on this computer on July 23, 2010. Mr. Lynch acknowledges that this occurred and that Stroz Friedberg was not provided with the other media where the 11

⁶ Lynch Expert Rpt. ¶ 27.

⁷ Lynch Expert Rpt. ¶ 28.

documents were created. Mr. Lynch then states that “older last modified dates show that these Draft Guerra Orders existed before July 2010”⁸ implying that Guerra authored these documents. However, there is no way to determine where these 11 documents were created or by whom. There is no forensic information regarding these conclusions provided by Mr. Lynch. In fact, it is just as likely that these documents were copied by former Judge Guerra from a computer at the Lago Agrio Court to the Western Digital hard drive, and from there to the Guerra computer.

32. Mr. Lynch also provided certain metadata fields for the 11 documents relating to the Lago Agrio Litigation. However, the metadata provided in the Lynch October Report is not the full metadata available for each document. Indeed, Mr. Lynch failed to identify certain properties of these fields that call into question the possibility that former Judge Guerra authored the reviewed documents — specifically the Author and the Company fields. These fields can indicate the identity of the computer on which the documents were created, and Mr. Lynch fails to provide any analysis regarding this aspect of identifying the actual author of these documents.

33. When reviewing both the original Author and the Last Saved By metadata fields found within the 11 documents relating to the Lago Agrio Litigation, it is clear these documents were created and last saved on a computer with Microsoft Office registered to the user ‘Usuario’. This indicates that the 11 documents were initially created on a computer that neither I, nor Mr. Lynch, have included in our analysis. There is no forensic evidence offered to show that former Judge Guerra ever used the computer with

⁸ Lynch Expert Rpt. ¶ 15.

Microsoft Office registered to the user 'Usuario' to author any documents, let alone these 11.

34. The evidence does indicate that the 11 documents identified in the Lynch October Report were created on a different computer than the one reviewed by Mr. Lynch. The Author name on the Guerra Computer is 'Estacion,' which is obviously different from 'Usuario.'⁹

C. MR. LYNCH'S ATTEMPTED AUTHENTICATION OF THE 105 DOCUMENT SET

35. Mr. Lynch also identifies an additional 105 other documents that do not relate to the Lago Agrio Litigation and attempts to 'authenticate' these documents and compare these documents to Ecuadorian court orders.

36. As stated above, there are significant questions with regards to the Chain of Custody of both the images and the 105 documents that exist on the Guerra media that Mr. Lynch did not adequately address. I have not seen any Chain of Custody documentation that demonstrates that the images that Mr. Lynch reviewed were in fact owned by former Judge Guerra. This lack of Chain of Custody should at least be addressed with regards to the authentication of the data on the media. Mr. Lynch can only address the Chain of custody from the time when the image was made. Without any further documentation, this exists as of July 15, 2013.

37. Additionally, the metadata of the 105 documents shows that all 105 files were last accessed on July 13, 2012 after 2:53 pm, the day that this media purportedly left

⁹ This information is found in the Registry 12-9017_Q10-Maxtor HD 6QZ3QWJM\C\Documents and Settings\Usuario\NTUSER.DAT\NTRegistry\\$\$\$PROTO.HIV\Software\Microsoft\Office\Common\UserInfo\UserName

the control of former Judge Guerra. This indicates that someone accessed these files just prior to the hard drive being shut down for the last time prior to imaging.

38. I also reviewed the available metadata for the 105 additional documents Mr. Lynch reviewed. Of these 105 documents, 103 have the Author set as “.”, i.e. a period. For the remaining two documents, the Author is listed as being registered to “Usuario” for one document, and “jtcivil” for one document. This indicates that the documents identified in the Lynch October Report were created on at least three separate computers as there are three different values for the Author field. The Guerra Computer that was provided has Estacion set for the Author entry and thus could not have been the original source of any of the 105 documents.

39. When reviewing the Author metadata field found within the 103 documents, it is clear these documents were created or originated from a computer registered to the user ‘.’. This indicates that these 103 documents were initially created on or came from a computer that neither I, nor Mr. Lynch, have in our possession. There is no forensic evidence offered to show that former Judge Guerra ever used the computer with Microsoft Office registered to the user ‘.’ to author documents.

40. This same analysis holds true for the remaining two documents with the Author field of ‘Usuario’ and ‘jtcivil’. This Author information indicates that these two documents were created on a computer or came from a computer that neither I, nor Mr. Lynch, have in our possession. There is no forensic evidence offered to show that former Judge Guerra ever used the computers with Microsoft Office registered to the users ‘Usuario’ or ‘jtcivil’.

41. The 105 documents have the user 'Estacion' listed as the user that last saved each of the documents. Review of the Registry of the Guerra computer shows that Microsoft Office is currently registered to the user 'Estacion'. This means that when the user of this computer saved a document, the user 'Estacion' would be listed as the user that last saved the document. However, while it is accurate to say that the metadata indicates that the documents were last saved on this computer (or one with the same Microsoft Word registration name), there is nothing to indicate what changes were made to the documents between creation and the last save. The documents could have been completely rewritten when last saved or they could have simply been looked at and saved to this computer.

42. I also performed analysis of the Author fields of all Microsoft Word documents that existed on the Guerra media. The chart attached as Exhibit C indicates all listed Authors for Microsoft Word documents found on the computer. This analysis shows that the vast majority of the documents that exist on the Guerra media were not originally created on the Guerra computer. In fact, based upon the review of the Guerra Computer Registry information, only the 34 documents with the Author information as 'Estacion' have Author information that matches Author information currently found in the Guerra Computer. The other approximately 1960 documents that exist on the Guerra Computer do not appear to have been authored on the Guerra computer.

43. Mr. Lynch claims, “[b]ased on the comparisons described above, the forensic evidence shows that the Court Website Documents were created from the Draft located on the Guerra Media.”¹⁰ However, the analysis that he relies on shows only that

¹⁰ Lynch Expert Rpt. ¶ 40.

the documents were textually similar and in some cases, have last save dates prior to when those documents were released by the Ecuador courts. This analysis does not prove that the documents found on the Guerra media were the original documents that the 105 orders came from, nor does it show if former Judge Guerra authored or modified these documents.

44. Mr. Lynch indicates that because in most of the 105 documents the Last Written Dates of the documents on the Guerra computer is prior the filing dates of the similar documents, this means that the documents on the Guerra computer are the source for the filed documents. However, Mr. Lynch also glosses over the fact that there are at least two instances where the Last Written Dates occur after the filling of the documents. This directly contradicts Mr. Lynch's conclusion that the Guerra documents are the source for the filed documents. Again, all this date shows is the moment in time when the document was last saved, not what content was added prior or by whom.

45. Mr. Lynch also describes the process he uses to compare the textual content of certain documents to orders found in the Ecuadorian court system. While Mr. Lynch's process does in fact do a comparison of these documents, the comparison of these documents is not an application of forensic science.

46. While technological in nature, the comparison done by Mr. Lynch is akin to simply reading two documents and identifying similarities and differences between these documents. This process does not require any forensic ability to perform.

47. Review of Mr. Lynch's analysis of the textual content of the 105 total documents in comparison to the Ecuador filings using off the shelf software appears to be relatively accurate with regards to the similarities between the documents. However,

nothing in the performed analysis indicates that the 105 documents were in fact drafts authored by former Judge Guerra.

48. In fact, there are at least two documents that have last written dates after the dates those documents were released by the Ecuador courts. These files have been highlighted on Exhibit O of Mr. Lynch's report and have been attached to this report as Exhibit D.

VII. CONCLUSION

49. Mr. Lynch concludes in his report that certain documents found on the Guerra Media were authored by former Judge Guerra and that these documents were the drafts of documents published by the Ecuadorian court system. However, the forensic evidence that Mr. Lynch cites to does not in fact support this conclusion. While the analysis he performs shows similarities between various documents, there is nothing that Mr. Lynch provides in his report that actually shows that former Judge Guerra was the author of any of the provided documents.



J. Christopher Racich, Esq.

President, Vestigant, LLC