Q: you were asked to perform a forensic examination of the computer in this case, is that correct?

A: yes

Q: according to your report, you used the forensic tools EnCase and IEF, is that right?

A: yes

Q: please explain for the court what EnCase is.

A: EnCase is a forensic tool capable of recovering deleted data and reviewing information on a computer. It is industry accepted as being one of the best forensic tools out there and has a legal journal of cases where it's been accepted in court

Q: So to make sure I understand, EnCase is a powerful forensic tool, capable of being used to recover and examine data from computer systems, correct?

A: yes

Q: would you be able to recover deleted pictures and videos within EnCase?

A: yes

Q: and you would also be able to recover system information, Internet history, and other types of data that show user activity, isn't that right?

A: yes

Q: what are some of the types of evidence that can be found on a computer using forensic tools that show user activity?

A: all kinds of stuff, Internet history, link files, volume shadow copies, Internet history - all of these and more allow us to timeline out and determine user activity.

Q: and the other tool you used, IEF, what does that acronym stand for?

A: Internet Evidence Finder

Q: and who makes that piece of software?

A: it is made by Magnet Forensics.

Q: is this a commonly used tool within the forensic community?

A: yes, almost all government and private labs use this tool.

Q: why did they use it?

A: most labs use it because it is a powerful forensic tool that is capable of recovering many types of artifacts and data, and it does so quickly without having to do it all by hand.

Q: would be fair to say that IEF recovers dozens, even hundreds, of different types of data from a computer and parses it out?

A: that is correct.

Q: and given the name of the software product, would be fair to say that it does recover a significant amount of Internet history records?

A: yes

Q: and these include deleted Internet history records, is that right?

A: yes

Q: in this case did you examine any Internet history records?

A: yes

Q: and did you prepare any of these records from the Internet history to include in your report?

A: yes

Q: what do these records relate to?

A: they are related to FedEx.

Q: and part of this evidence are Google searches, is that correct?

A: yes

Q: can you explain for the court with these records mean?

A: yes, these are times where a person actually search for FedEx using the Google search bar.

Q: and you also have something called par search queries, is that right?

A: yes

Q: how are these different than Google searches?

A: these are searches performed on the computer using applications other than Google, such as Bing or Yahoo search engines.

Q: all the records here for par search queries also relate to searches performed by a user of the computer then, is that correct?

A: yes

Q: and all the searches related to FedEx, is that right?

A: yes

Q: you also have Internet history records related to FedEx that you recovered in this report is that right?

A: yes that is correct.

Q: based upon the Internet history records and searches, can you tell what was contained in those packages?

A: no I cannot.

Q: based upon the Internet history records and searches, can you tell who those packages were sent to?

A: no

Q: based upon the Internet history records and searches, can you tell of those packages were successfully delivered?

A: no

Q: based upon the Internet history records, do you actually typed the searches into the computer?

A: no

Q: is it fair to say that using the forensic tools EnCase and IEF would allow you to recover hundreds of thousands, or even millions of records related to Internet usage?

A: yes

Q: does your report include all of the Internet history records recovered from the computer?

A: no

Q: does it include all the Google searches made on the computer?

A: no

Q: does it include all the parsed to search queries recovered from the computer?

A: no

Q: did you examine the computer for anything else other than FedEx records?

> IF YES: Q: and the only information of interest you found were these handful of records, is that correct?
>
> IF NO: Q: so by your own admission, no attempt was made to examine the computer for exculpatory evidence?

Q: did you attempt to subpoena FedEx for more information about the packages mentioned in your report?

A: no

Q: so you didn't think the company that actually transported these packages would have valuable information for your investigation?

A: wasn't relevant, etc.

Q: so a handful of searches on a computer, that by your own admission you can't tell who did them, what the content of the packages were, or were they were sent to, and information directly for FedEx would not be relevant?

A: ?

Q: is it possible FedEx would have exculpatory information?

A: end

END CROSS EXAM