

**Computer Forensics Expert**  
**VS**  
**Private Investigator**



**A Certified CSI, LLC White Paper**

*By David Jacquet*

*MCSE, CEH, CEI, CISSP*

*Certified CSI, LLC*

*President*

We don't wear Fedoras. We don't "pack heat". We don't conduct stakeouts in the middle of the night. We don't drive bright red Ferraris all over Hawaii. What we do is uncover digital evidence that slams cases shut.

Many think of Computer Forensics experts (CFE) as the 21st century version of the PI of yore. It is, in my opinion, a terrible comparison. Not that I have anything against Private Investigators or the work they perform - I don't. Simply put, a PI's daily activities and a CFE's daily activities have little, if anything, in common.

The actual, real-world practice of Computer Forensics is more technical than investigative in nature.

First of all, many of the activities that make up Computer Forensics are not investigative at all. Such tasks include disk duplication, lost password retrieval and deleted files recovery.

More often than not, the involvement of the Computer Forensics expert only occurs as the result of an on-going investigation carried on by a third party – not by the CF expert. In other words, the CFE does not set out to investigate an individual. That decision is taken by someone else, who then proceeds with their investigation. During said investigation, this third party may decide that a hard drive, a computer, or any other digital media may contain information that would pertain to the investigation, and require the services of a CF expert. A CFE provides technical expertise in a supporting role to an on-going investigation.

Note that:

1. Situation-relevant information may not be found on the provided media
- 2.If information is found, it may be inculpatory or exculpatory, i.e. it may reinforce or invalidate the original investigation carried on by the third party. Either way, the CF expert will, if required, testify to what they found, regardless of the impact it may have on the situation/case.
- 3.The way in which the information is discovered always abides to standards of court admissibility.
- 4.The CF expert does NOT act upon the information discovered during the forensic examination. If action is required based on the situation, the investigating third party would carry it on with no further involvement from the CF expert.

In other words, it is an accurate description of CF activity to say that:

- 1.Many CF tasks are completely non-investigative in nature.
- 2.The CF expert does NOT provide /seize the media. It is brought to them by a third party.

3.The CF expert's involvement is limited to the technical search and potential retrieval of information on the provided digital media.

4.The information found may advance the investigation or not.

5.The CF expert's responsibility is to present ANY information discovered, regardless of the impact of this information on the investigation.

6.The CF expert does NOT act upon the information discovered, but instead passes it along to the investigative third-party that hired them.

7.The CF Expert's responsibility is to technically uncover information on a provided piece of digital media in such a fashion as to:

a. Not delete or change any of the information.

b. Make sure that any information discovered is admissible in a court of law.

*About the Author:*

David Jacquet is the President of Certified CSI, LLC. David has 10 years of experience working in IT. His past employment includes positions as Network Engineer, Microsoft Certified Trainer, Network Security Engineer, Information Security Trainer, Director of Content Development, and Director of Security Education Services.

David has delivered many public speaking engagements on such topics as Phishing, E-commerce and Identity Theft, and Ethical Hacking.

David holds many IT certifications, including Microsoft's MCSE, Cisco's CCNA, EC Council's CEH and CEI, and ISC2's CISSP.

David has authored 12 IT books, and is the co-author of Security Policies and Procedures published by McGraw-Hill.

Prior to working in IT, David taught at such Institutions of Higher Learning as the Massachusetts Institute of Technology in Cambridge, MA, Bowdoin College in Brunswick, ME, and the Naval Academy. David still holds the rank of Lieutenant.