**Week 6 Project: Analysis of Computer Forensics Code of Ethics**

**And possible ethical issues**

By Matthew Ferry

June 11, 2011

Table of Contents

[Introduction 3](#_Toc295590080)

[Computer Forensics 4](#_Toc295590081)

[Code of Ethics 5](#_Toc295590082)

[CCE (*Code of Ethics and Professional Responsibility*. 2011) 5](#_Toc295590083)

[CFCE (*New Membership: Code of Ethics*. 2011) 6](#_Toc295590084)

[Possible Ethical Issues 7](#_Toc295590085)

[Differences between Corporate and Legal views: 7](#_Toc295590086)

[Abuse of Access: 7](#_Toc295590087)

[Fourth Amendment Issues: 8](#_Toc295590088)

[Maintaining Data Integrity: 8](#_Toc295590089)

[Summary 9](#_Toc295590090)

[References 10](#_Toc295590091)

# Introduction

Considering that the field of “Computer Forensics” is still being defined in today’s world, this field is currently very challenging in regards to ethical decisions that must be made by the computer investigator. This challenge presents itself in the upholding of ethical codes that must be upheld in order to qualify for possible required certifications, and in other ethical issues that may present themselves.

Two common certifications of CCE and CFCE have been listed in this report, along with a copy of their respective Ethical codes.

Four possible ethical dilemmas that a computer forensics investigator may encounter are also briefly covered, and why these issues are important for the investigator to constantly be mindful. Those dilemmas are: 1) Differences between Corporate and Legal views, 2) Abuse of access, 3) Fourth Amendment Issues, and 4) Maintaining Data Integrity.

# Computer Forensics

The current intended focus of my college studies is that of Computer Information Systems with a focus in Computer Forensics.

What makes this a profession is that as technology levels continue to advance, it is becoming easier and easier to be abused by people that see no ethical issue in taking advantage of the flaws in technology. As such, these people are furthering their own goals and agenda’s but at the expense of breaking the law, and since they do not want to be caught, they are willing to do anything they can to cover their trails and destroy digital evidence that could be used against them.

This is the overall goal of someone in the field of Computer Forensics. Discover the unwanted trails and digital evidence that has been left behind, which shows proof of illegal activity, and depending upon the type and extent of the investigation, the discovery of flaws that made the illegal activity possible.

Ten years ago, there were no real degrees or certifications for this particular profession, but throughout the years as the need for qualified individuals has continued to climb certifications and other credential based qualifications have been implemented.

## 

## Code of Ethics

The certifications required will vary per specific job description however; the most common certifications that I have found are CCE (Certified Computer Examiner) or CFCE (Certificate Forensics Computer Examiner) certifications. Both of these certifications have a code of ethics that certified holders must follow.

### CCE (*Code of Ethics and Professional Responsibility*. 2011)

**A Certified Computer Examiner will at all times:**

* Demonstrate commitment and diligence in performance of assigned duties
* Demonstrate integrity in completing professional assignments
* Maintain the utmost objectivity in all forensic examinations and accurately present findings
* Conduct examinations based on established, validated procedures
* Abide by the highest moral and ethical standards and abide by the Code of the ISFCE
* Testify truthfully in all matters before any board, court or proceeding
* Avoid any action that would knowingly present a conflict of interest
* Comply with all legal orders of the courts
* Thoroughly examine all evidence within the scope of the engagement

**A Certified Computer Examiner will never:**

* Withhold any relevant evidence
* Reveal any confidential matters or knowledge learned in an examination without an order from a court of competent jurisdiction or with the express permission of the client
* Express an opinion on the guilt or innocence of any party
* Engage in any unethical or illegal conduct
* Knowingly undertake an assignment beyond his or her ability
* Misrepresent education, training or credentials
* Show bias or prejudice in findings or examinations
* Exceed authorization in conducting examinations

### CFCE (*New Membership: Code of Ethics*. 2011)

**Members must:**

* Maintain the highest level of objectivity in all forensic examinations and accurately present the facts involved.
* Thoroughly examine and analyze the evidence in a case.
* Conduct examinations based upon established, validated principles.
* Render opinions having a basis that is demonstratively reasonable.
* Not withhold any findings, whether inculpatory or exculpatory, that would cause the facts of a case to be misrepresented or distorted.
* Never misrepresent credentials, education, training, and experience or membership status.
* Advise and provide assistance to all qualified IACIS® forensic examiners, regardless of agency affiliation.

## Possible Ethical Issues

Some ethical issues within this field are 1) Differences between Corporate and Legal views, 2) Abuse of access, 3) Fourth amendment Issues, and 4) Maintaining Data Integrity.

### Differences between Corporate and Legal views:

Different views between corporate and legal views and the reporting of issues can easily be an ethical dilemma for someone in the field of computer forensics. This is because the different views have different priorities. Corporations focus on detecting, minimizing, and preventing unauthorized or inappropriate computer usage, while the Law focuses on investigating and prosecuting according to the appropriate state or federal laws (Basset, R, Bass, L., & O’Brien, P. 2006). This is an issue because someone in the forensics field may very easily find themselves faced with a situation where the examiner feels compelled to report something to the authorities, yet the corporate policy for the corporation that employees him is not to report the situation due to further legal ramifications that the corporation wants to avoid.

### Abuse of Access:

An article published late last year in the American Journal of Business Education (Brooks, R. 2010), goes into an in depth look at “computer ethics and the lack thereof” in general, and briefly discusses issues that exist because of this. One of these issues is the abuse of access that thousands of IT professionals commit every year, as they read confidential files, and access computers without permission, and this trend is growing, primarily due to a lack of computer ethics. This can provide someone in the field of computer forensics with a possible ethical dilemma because in order to examine almost any computer situation administrator or root access is required. As such, they will constantly face the temptation of looking into other areas that are not directly connected to their current investigation.

### Fourth Amendment Issues:

A computer forensics specialist that works with law enforcement also has ethical and legal issues of making sure that no fourth amendment rights are violated during the obtaining of any type of digital evidence (Grama, J. L. 2010). This is because evidence that is obtained without the proper authorizations and warrants will be considered in admissible in court, which will essentially invalidate the work that was done in obtaining the evidence. This is an ethical issue, because when obtaining search warrants, the rules for the search criteria are extremely specific, and any violation of that search criteria could invalidate evidence found. Thus, it is important for the computer examiner to only be looking for information regarding the current investigation. Any other legal questions that may be accidently uncovered should immediately be addressed from the standpoint of obtaining the proper warrants to continue to look into the new issue.

### Maintaining Data Integrity:

During any investigation process, the process of maintaining data integrity is extremely important as any accidental data manipulation could invalidate the admissibility of the data in question (Stewart, James Michael & Tittle, Ed & Chapple, Mike. 2008). The ethical dilemma here is what does the investigator do if a mistake is made? Even if a mistake is made, and reversed the integrity of the data has already been compromised, and if questioned under oath about the integrity it would unethical to lie about the integrity. This is why the importance of data imaging and hash or md5 sum verification is so important. This process allows the investigator to maintain original data integrity, and verify that throughout the examination process that data integrity has been maintained.

## Summary

As the field of Computer Forensics is a very specialized field, it is clear by the ethical issues listed in this report, that working within this field has the possibility to be extremely challenging due to the frequency of possible ethical pitfalls. However, it is also clear that strict adherence to a code of ethics and investigation procedures and policies will greatly reduce the temptation or consequences of any ethical pitfalls.

# References

Bassett, R., Bass, L., & O'Brien, P. (2006). Computer Forensics: An Essential Ingredient for Cyber Security. *Journal of Information Science & Technology*, 3(1), 22-32. Retrieved June 11, 201,1 from EBSCO*host*.

Brooks, R. (2010). The Development Of A Code Of Ethics: An Online Classroom Approach To Making Connections Between Ethical Foundations And The Challenges Presented By Information Technology. *American Journal of Business Education*, 3(10), 1-13. Retrieved June 11, 2011, from EBSCO*host*.

*Code of Ethics and Professional Responsibility*. (2011). Retrieved 06 11, 2011, from The International Society of Forensic Computer Examiners: http://www.isfce.com/ethics2.htm

Grama, J. L. (2010). *Legal Issues in Information Security.* Jones & Bartlett Learning. Retrieved June 11, 2011 from EBSCO*host*.

*New Membership: Code of Ethics*. (2011). Retrieved 06 11, 2011, from The International Association of Computer Investivative Specialists: https://www.iacis.com/new\_membership/code\_of\_ethics

Stewart, James Michael & Tittel, Ed & Chapple, Mike. ( © 2008). Cissp: certified information systems security professional study guide, fourth edition. [Books24x7 version] Available from http://common.books24x7.com.proxy.devry.edu/toc.aspx?bookid=25182.