

# Ethics of kevin mitnick and computer hacking philosophy essay



**ASSIGN  
BUSTER**

This discussion paper is about Kevin Mitnick and Computer Hacking. It is divided into two sections. The first section discusses the life of Kevin Mitnick in relation to computer hacking. It highlights the ethical issues involved during his various computer crimes, police investigations, arrests and imprisonments. It also applies ethical theories to discuss the FBI attempt to capture and prosecute Mitnick. The second section of this paper discusses the role of a professional software/hardware/application engineer with regard to hacking. It discusses how such an engineer should use his/her knowledge and expertise to influence the society. It looks into the different possible roles and suggests the role that such a professional engineer should play.

## **Ethical Issues**

The case of Kevin Mitnick was a controversial one which brings to light many ethical issues. These can be seen from the way Mitnick illegal hacked into computer systems, down to the way the FBI and the Federal Government attempted to track him down. Some of the issues are discussed below:

1) Kevin Mitnick grew up without the opportunity to have a good moral training and development on ethical values. Mitnick grew up a lonely kid. His dad split with his mum when he was three years old. His mother then had to work as a waitress in order to support them. He was an only child being raised by a mother who put in long harried days on a sometimes-erratic schedule. That saw Mitnick as a youngster on his own almost all his waking hours. He was his own baby sitter [1]. This exposed him to the ills of the society at a very young age. Growing up in a San Fernando Valley community gave him the whole of Los Angeles to explore. This didn't give him the opportunity to have proper moral training and acquire good habits

<https://assignbuster.com/ethics-of-kevin-mitnick-and-computer-hacking-philosophy-essay/>

and character traits needed to develop to be a moral person. Moral training and development is very essential in the life of every individual. A moral person is necessarily disposed to do the right thing [2]. Since Kevin lacked the necessary parental training needed to develop to be a moral person, he was necessarily disposed to do the wrong things. This greatly affected the decisions he made in life. He was bound to make several wrong decisions when it involved ethical considerations. At the age of twelve, he already made the first of such decisions as he learned to a way to travel free throughout the whole greater L. A. area. This was a major step on his road to becoming a computer hacker. Had Kevin Mitnick had proper parental and moral upbringing, he probably would have turned out to be a different person, free of computer crimes.

2) Was it ethical for Kevin Mitnick to use his computer expertise to invade on the autonomy of various individuals and organisations? Mitnick hacked into several computer systems of various companies and organizations, thereby breaching their autonomy. Autonomy is one of the core values in every society. Everyone has the right to enjoy autonomy. Kevin mainly used social engineering to get the information needed to hack into these computer systems. In an interview with CNN in October 2005, Mpppppppppitnick defined social engineering as follows “ Social Engineering is using manipulation, influence and deception to get a person, a trusted insider within an organization, to comply with a request, and the request is usually to release information or to perform some sort of action item that benefits that attacker. It could be something as simple as talking over the telephone to something as complex as getting a target to visit a website, which exploits

a technical flaw and allows the hacker to take over the “[3]. Mitnick used the art of deception to achieve his goals. He hacked into computer systems of several innocent organizations causing different types of damages. Many of the affected organizations were forced to spend lots of money to just detect how he was able to hack into the computer system. They still went on to spend more money on developing better security solutions. All these were caused by Mitnick invading on their autonomy. Even though Mitnick might claim that many of his misdeeds were motivated by curiosity, the fact remains that the actions he took were illegal, and that he committed invasions of privacy. This was very unethical.

3) Was it ethical for John Markoff to publish many stories on Kevin Mitnick without the necessary evidence to back it up? John Markoff, a reputable journalist wrote several articles and books on Kevin Mitnick containing different stories, many of which the sources were not cited. Markoff wrote articles such as “ Combining technical wizardry with the ages-old guile of a grafter, Kevin Mitnick is a computer programmer run amok” (the New York Times, 7/4/94) and a book in 1991 called, Cyberpunk. These stories were used to turn the image of Mitnick in to Public Enemy number one of cyberspace [1]. Markoff mainly wrote and published these stories for his own personal financial gain. He became a millionaire by writing false stories of about Mitnick without appropriate evidence. Some of the most famous stories were the ones which Markoff claimed Mitnick had wire tapped the FBI and also broken into the computers at North American Air Defense Command (NORAD) [1]. These stories were not backed up with evidence and were used to paint a bad image of Mitnick, while Markoff gained financially.

All these were achievable because most people trusted stories published in the pages of the New York Times. This actually changed the world's perception of the danger Mitnick represented [1]. Mitnick then became one of the most feared men in the United States. Markoff was merely using Mitnick as a means to an end, which was financial gain. Markoff used the same technique Mitnick used on people, which was deception. Markoff used the act of deception to become very famous and rich. He did not treat case of Mitnick universally, like he treated other stories. He saw the opportunity to benefit financially and exploited it. This was really unethical. Markoff was a professional journalist whose duty to the public was to seek the truth and report it. His obligation was to be honest, fair and courageous in gathering, reporting and interpreting information. This is what was expected of professional journalists, especially reputable ones like Markoff. He certainly failed in this duty.

4) Were the FBI and the Federal Government ethical in they manner they treated the Kevin Mitnick case? The way they treated the case of Mitnick was very controversial. His treatment was not universal, but partial. The FBI and the Federal Government did not treat other cases of computer hackers in the same way. Mitnick was treated like a terrorist or violent criminal. There were many things which the FBI did in their attempt to arrest Mitnick that raised eyebrows. His residence was searched with a blank search warrant, he was thrown into solitary confinements for months, he was denied not only bail but a bail hearing and was forced to spend years fighting to obtain the government's evidence, so the court appointed attorney could prepare his defense [1]. This was not the way other computer hackers were treated.

Only terrorists and violent criminals were treated this way. Mitnick was just a mere computer hacker whose crimes were simple crimes of computer trespass and making free telephone calls. It was more like the Federal Government were trying to make an example of him not based on the crimes he committed. His case had been over hyped by the media to a level where the government could not afford to lose. This might have been why they did all they could to capture Mitnick. He was placed in solitary confinement because law enforcement officials convinced a judge that Mitnick had the ability to 'start a nuclear war by whistling into a payphone' [4]. This, in common sense sounds quite ridiculous. But this was the extent to which the FBI went in the Mitnick case. This was certainly non-universal and partial. Computer hackers were not normally treated this way. This really poses an ethical issue.

5) Was Tsumoto Shimomura involvement in the capture of Kevin Mitnick ethical? Shimomura helped the FBI trace and capture Mitnick for his own personal satisfaction. "On Christmas Day, 1994, a hacker launched a sophisticated 'IP Spoofing' attack against Tsumoto Shimomura's computers in San Diego. The attack was launched from toad.com in San Francisco, the Toad Hall computer owned by John Gilmore, a founding employee of Sun Microsystems. By an uncanny coincidence, Shimomura spent the day at Toad Hall with his friend Julia Menapace. Shimomura's pursuit of the hacker led to computers in Marin County where Shimomura's stolen files were found on The Well, Denver, San Jose and finally to Kevin Mitnick, the fugitive hacker, in Raleigh, North Carolina[5]. This attack greatly angered Shimomura as he was also a computer expert and must have felt embarrassed that even

his own computer could be hacked into. Shimomura helped the FBI track Mitnick down less than two months after then. As a computer expert, Shimomura must have known about Mitnick and his computer crimes. He would have known the FBI had been trying to track Mitnick down without success. But he never offered to help. If Shimomura was thinking of the greater good of the society, he would have helped the FBI before his own computer was attacked. Shimomura took this attack by Mitnick as a personal challenge. He did not help the FBI innocently, but to attain his own personal satisfaction of apprehending the man who attacked his computers. Had Mitnick not attacked Shimomura's computers, Shimomura will probably not have helped the FBI track Mitnick down. Shimomura should have been thinking about doing the right thing rather than just achieving his own personal happiness. Also, it is still unclear whether Shimomura's involvements followed the proper legal procedures [6]. John Markoff and Tsutomu Shimomura both participated as de facto government agents in Kevin Mitnick's arrest, in violation of both federal law and journalistic ethics.

6) Was it ethical for the Federal Government to make a new Federal Law which was nonsystematic and non-comprehensive and then charge Kevin Mitnick under it? The new Federal law made it a crime to gain access to an inner state computer network for criminal purposes. What is the real question here? Is it about gaining access to an inner state network or is it about the crime in getting into any computer network for criminal purposes. An ideal law is not merely reactive to a particular incident, nor is it one that is hastily passed because it happens to involve prominent person rather than ordinary citizens [2]. This is what happened in the Mitnick case. The new law

was specific to the inner state computer networks. The Federal Government made this law hastily in order to be able to charge Kevin Mitnick with it. The law was neither comprehensive nor systematic. It did not cover other classes of the society which also had computer networks that could also be hacked into. The passing of this new law definitely raises an ethical issue. It only protected the inner states computer networks but left out the rest of the other computer networks in the society.

## **Ethical Theories**

There have been many debates on the ethical behavior of the FBI in this case. Many people say the FBI acted ethically while others disagree. Various ethical theories can be applied to determine whether the FBI was correct in attempting to capture and prosecute Kevin Mitnick.

Consequence Based Theories (Utilitarianism):

Consequence-based ethical theories focus on producing desirable outcomes. Applying these theories to this case, one can conclude that the FBI was correct in their attempt to capture and prosecute Kevin Mitnick. Utilitarians argue consequences of the greatest number of individuals, or the majority, in a given society deserves consideration in moral deliberation [2]. Mitnick was a computer hacker who gained access into several computer systems belonging to various organizations and establishments for illegal purposes. He was a security threat to any computer network in the United States. No one could predict which computer network he will hack into next or which information he will tamper with next. Capturing and prosecuting him brought satisfaction to the majority of people in the United States. Looking at it from



the perspective of Act Utilitarianism, " Act X, is morally permissible if consequences produced by doing X result in the greatest good for the greatest number of persons affected by X" [2]. The important point here is the greatest good for the greatest number of persons. The majority of Americans are affected by computer networks either directly or indirectly. Those that own computer networks or work in organizations having computer networks are directly affected by any harm Mitnick inflicts on such a network. Organisations have various types of information stores or processed by computer systems. Any compromise to such information could cost a lot of damages in terms of money and reputation. Having the assurance that such data is safe or that any one who attempts to illegal access it is prosecuted by the law brings some sense of satisfaction and happiness to such an organization or individual. All other people are indirectly affected as majority has their data stored in various organization and states computer systems. These computer systems hold databases of various types of data such as telephone bills, tax payments and much more. Having the assurance that these databases are secure or that anyone illegal hacker is brought to justice certainly brings a sense of satisfaction and happiness to the people involved which is the majority of people in the United States in this case. Therefore by applying act utilitarianism to the case of Mitnick, the FBI were correct in attempting to capture and prosecute Mitnick as this brought happiness to the majority of people living in the United states. This fulfils the conditions in Consequence based theories.

Duty-Based Ethical Theories (Deontology):

Applying Duty Based ethical theories to the case of Kevin Mitnick, one can argue that the FBI was correct in attempting to capture and prosecute Mitnick. Duty based ethical theories base morality on concept of duty or obligations humans have to one another. Morality should never be grounded in consequences of human actions. It had nothing to do with the promotion of happiness or attaining desirable consequences [2]. The question here is whether it was the duty of the FBI to attempt to capture and prosecute Mitnick. The Federal Bureau of Investigation(FBI) is law enforcement and domestic intelligence agency charged with protecting and defending the United States against and foreign threats; upholding and enforcing the criminal laws of the United States; and providing leadership and criminal justice services to Federal, State, Municipal and International agencies and partners [7]. It was obviously the duty of the FBI to protect the United States from people like Mitnick. Mitnick was a computer hacker with so much expertise that he posed a security threat to the United States. It was rumored that Mitnik hacked into the computers of NORAD in Colorado Springs. NORAD was part of a Military Defense System in which any damage or compromise to its information could have catastrophic effects. It was also rumored that Mitnick had wiretapped the FBI. Even though evidence for these allegations never surfaced, it was obvious that Mitnick had become a security threat. The FBI owed the people of the United States the duty or obligation to track down people like Kevin Mitnick. Even though the manner in which the FBI went about this duty is questionable, that does not take away the fact that it was their obligation to the people of the United States. If we consider the manner in which the FBI went about the Mitnick case, one can say that it was unethical. Duty-based ethical theories are based on the <https://assignbuster.com/ethics-of-kevin-mitnick-and-computer-hacking-philosophy-essay/>

grounds that humans are rational, autonomous agents and ends in themselves and not as a means to ends. Kevin Mitnick was treated as a means to an end. Because of the media hype that had developed on Mitnick and his computer crimes, the FBI wanted to apprehend Mitnick by all means for the sake of their reputation. The FBI did not treat the case of Mitnick universally. Other computer hackers were not treated this way. During the case of Mitnick, many things peculiar to his case were done. These involved searching his house with a blank search warrant, formulation of a new Federal law and charging him with it, putting him in the hole-solitary confinement, denying him the right to a bail hearing and many more. The FBI did not approach other cases of illegal computer hacking in similar fashion. Under Rule Deontology, same rules should apply universally to all persons. This was certainly not the case for Kevin Mitnick. Mitnick was not treated universally like other computer hackers. He was used as a means to an end, which was to uphold the reputation of the FBI.

Even though the manner in which the FBI went about this duty is questionable, it does not take away the fact that it was their obligation to the people of the United States. Since we are considering whether the FBI were correct in attempting to capture and prosecute Mitnick and not the procedures the FBI used in achieving this, one can conclude that the FBI were correct. This was a duty which the FBI owed to the people of the United States of America.

Character Based Ethical Theories (Virtue Ethics):

Applying Character Based Ethical theories to the case of Kevin Mitnick is quite difficult. These theories focus on criteria having to do with the character development of individuals and their acquisition of good character traits from the kinds of habits they develop. But these theories have better chance of being implemented in a society that is homogeneous rather than a heterogeneous society. In contemporary America, which is much more heterogeneous than classical Greek society, we have a diversity of views about which ideas and values are most important [2]. Kevin Mitnick grew up in the contemporary America. As I pointed out earlier, Mitnick grew up a lonely kid. He was raised by his mother whom usually worked long hours to be able to support them. He did not have proper training and acquisition of good habits and character traits for him to achieve right moral virtues (strengths and weaknesses) as required in a character based ethical system. These ethical systems tend not to flourish in society in which Mitnick grew up which places emphasis on the importance of individual autonomy and individual rights. A moral person is necessarily disposed to do the right thing. Hence, one can say that Mitnick was necessarily disposed to do the wrong thing. Therefore it is difficult to apply character based ethical theories to discuss whether the FBI was correct in attempting to capture and prosecute Kevin Mitnick. These ethical theories place emphasis on moral development and moral education based on homogeneous community standards. This doesn't apply to the case of Mitnick, because he grew up in the contemporary America which is a heterogeneous community.

## **The Role of a Professional Software/Hardware/Application Engineer**

The role of a professional software/hardware/application engineer is a very critical one. The knowledge and expertise within their disposal gives them the capacity to access and manipulate various levels of information. This could be used positively or negatively. Don Gotterbarn (2001) believes software engineers and their teams have significant opportunities to do good or cause harm, to enable others to do good or cause harm and to influence others to do good or cause harm [2]. Many of such professional engineers use their knowledge to hack into various types of computer systems for various purposes. Some do it to achieve some form of financial gain and others do it for their own personal satisfaction. This should not be the case. Professional Engineers have a duty to do good in every situation. They ought to follow the Code of Ethics of the professional organization to which they are affiliated. This Code of Ethics always discourages every form of ill-doing and tends to promote the greater good of the society. Implementation of this code of ethics is often the problem. Even though there are documented disciplinary actions against those who breach any of these rules, it happens very rarely. This gives many of these professionals the liberty to do whatever they wish.

Looking further into the life of Kevin Mitnick, I found out that he now runs Mitnick Security Consulting LLC, a computer security consultancy. The company offers a comprehensive range of services to help businesses protect their valuable assets [8]. Mitnick has also written a few books such as “ The Art of Intrusion” and “ The Art of Deception” [6]. These books help

educate readers on the various methods hackers use to achieve their goals and suggest different ways to guard against such attacks. Based on his previous life style, Mitnick discussed the various techniques he used to succeed in his computer crimes. His company specialized in providing security solutions. Several organisations and individuals employed the services of his company to analyse their computer networks and implement better security solutions. Mitnick also presents speeches in various seminars and workshops around the world. He goes around trying to educate people on the dangers in computer hacking. He also attends several radio and television interviews. He is trying his best to use his computer expertise to affect the world positively. He is now doing the exact opposite of what his former life style. This is the role expected of a professional software/hardware/application engineer.

The life of Kevin David Mitnick is a good example that portrays two different roles for such professionals. The first phase of his life was a negative role where he used his knowledge to achieve his own selfish ambitions while causing a lot to damage to various organizations. The second phase of his life is a role in which he is making a positive impact to the society at large. In this role, a professional software/hardware/application engineer uses his knowledge and expertise to educate the society on the various techniques used by hackers and how to guard against them. The engineer produces various types of security solutions to enable organizations secure confidential information and makes many more positive contributions to the society.

Tsutomu Shimomura is another good example of a computer professional who has been affecting his society positively. Shimomura has also worked in the area of computer security research. He has consulted with a number of government agencies on security and computer crime issues. In 1992 he testified before a Congressional Committee chaired by Representative Edward Markey on issues surrounding the lack of privacy and security in cellular telephones. In February 1995 he helped several online service and Internet companies track down computer outlaw Kevin Mitnick, who had stolen software and electronic mail from Shimomura's computers [9]. As we can see, Shimomura even helped the FBI track down and capture Mitnick, the notorious computer hacker. Shimomura has affected his society positively on several occasions. This again is an example of what is expected of a professional software/hardware/application engineer.

Computer hacking for illegal purposes is a crime and is ethical wrong. It should be discouraged at every level in the society. Professional software/hardware/application engineers ought not to engage in such practices, but use their expertise to promote the greater good of the society. They have significant opportunities to do good or cause harm. But their duty to the society is to use their knowledge to do good always.

## **Conclusion**

Kevin Mitnick is a name that will definitely not be forgotten for many years to come. He will be remembered as one of the most notorious computer hackers in American History. Even though most of his computer crimes were not malicious and not on safety-critical systems, most of his actions were unethical. He violated the core values of happiness and autonomy. The FBI  
<https://assignbuster.com/ethics-of-kevin-mitnick-and-computer-hacking-philosophy-essay/>

was definitely right in attempting to capture and prosecute him, even though many of their actions were also unethical. They treated Mitnick as a means to an end and not as an end himself. The present lifestyle of Kevin Mitnick is a good example of the general role a professional software/hardware/application engineer should play in terms of the use of their knowledge and expertise in regards to hacking. This use of this knowledge and expertise should be for the greater good of the society.