Spring 2019

What the hack is a hacker?

Paige Franklin

Ryan Adams

Caroline Henry

What the Hack is a Hacker?

An Honors College Project Presented to

the Faculty of the Honors College

James Madison University

by Paige Marie Franklin, Ryan Edward Adams, and Caroline Carson Henry

May 2019

Accepted by the faculty of the Honors College, James Madison University, in partial fulfillment of the requirements for the Honors College.

FACULTY COMMITTEE:

Project Advisor: Philip L. Frana, Ph.D.,
Associate Dean, Honors College

Reader: Jim E. Lantzy, D.A.,
Adjunct Professor, Computer Information Systems

Reader: David L. Hardy, M.F.A.,
Assistant Professor, Graphic Design

HONORS COLLEGE APPROVAL:

Bradley R. Newcomer, Ph.D.,
Dean, Honors College

PUBLIC PRESENTATION

This work is accepted for presentation, in part or in full, at Honors Symposium on April 5, 2019.

Acknowledgements

The authors of this paper would like to extend our sincerest thanks to our project advisor, Dr. Philip Frana, for his unwavering guidance and support throughout this entire process. Dr. Frana not only inspired this project, but he kept our morale high throughout the entirety of its completion. We could not be more thankful for him or the time, energy, and effort he has dedicated to ensuring that this project was of the highest quality possible. We would also like to thank our project readers, Dr. Jim Lantzy and Professor David Hardy, for dedicating their time to providing us with invaluable feedback on our project. Finally, we would like to thank the entire faculty and staff of James Madison University's Honors College for supporting us in this endeavor and pushing us to produce a work we are proud of.

Abstract

The purpose of this study is to examine the historical tendencies and characteristics of hackers to create a holistic definition of what it means to be a hacker. By analyzing the contents of the "Hacker Classics" list, it was determined that there is not a single, all-encompassing definition of what it means to be a hacker. Although there are common motivations and ideologies between many hackers, the definition of "hacker" continues to change as time and technology does.

Table of Contents

Introduction

The history of computer programming now dates back more than fifty years. In that time, thousands of articles have been published online that are of interest to hackers. So many articles, in fact, that the hacker community has had to develop some ways to get a handle on all the information available to them. And what better way than through collaborative filtering, a process that collects ratings from members of the hacker community? What is there to gain from a list of upvoted articles compiled by an algorithm? What is the point of such a list? What can a list like this tell us about human professions, innovation, historical trends, and how the world works? What does a list titled "Hacker Classics" mean to people who identify as hackers?

Historically and generally, the computer science and programming communities are future-focused. Their innovations and work are geared towards moving today's society to the next step in time and technology. But the "Hacker Classics" list (http://jsomers.net/hn/) explores the history of the information/technological revolution and the people behind it. Upon viewing this list, we wondered if it could serve as a way that hackers and programmers are attempting to understand where they came from and what forces have influenced the hacker community and their work over time?

The questions stated above were just a few of our initial thoughts when we first examined the "Hacker Classics" list. We were intrigued by this list of articles, journals, video links, and scholastic essays engineered by a group of hackers. This interest in understanding the meaning behind the “Hacker Classics” list sparked a deep dive into primary sources and research, that when considered as a whole, creates a holistic picture of hackers and the hacking community.

Y Combinator

Y Combinator is an investment company started in March 2005 by Paul Graham and Robert Morris, along with Jessica Livingston and Trevor Blackwell (People). The company has invested in over 1,450 companies, including Airbnb, Reddit, and Dropbox (Bio). In return for investing in companies, Y Combinator requests a percentage of equity (About Y Combinator). The company went global in 2016, as they began to meet with investors and entrepreneurs in 11 countries (Manalac, 2016). In addition to investing in startups, Y Combinator currently runs *Hacker News* and hosts the “Hacker Classics” online list.

Hacker News

Hacker News is a news aggregator site with the purpose to present “anything that gratifies one’s intellectual curiosity,” (Graham, Startup Becomes Hacker News). It was published on February 17, 2007 by Paul Graham (Rao, 2013). The format of *Hacker News* is based on a reputation economy that closely mirrors that of Reddit, as there are multiple listings on each page which users can upvote (Graham, Hacker News FAQ). However, *Hacker News* differs from Reddit in that there is no option to down-vote a listing.

Anyone who has registered on the site and selected a username can submit content to *Hacker News*. When a listing receives enough points, it becomes visible on the homepage of the site (Graham, Hacker News FAQ). The listings change frequently based on the number of points received. Points are derived from the number of upvotes divided by the number of hours that the post has been displayed on the site. There are also other, undisclosed factors that are considered by the algorithm to determine the rankings of the listings on the site (Graham, Hacker News FAQ). These additional factors may include the number of clicks on each listing or the number of comments a listing receives.

Hacker News states that users who submit listings cannot request that other people upvote their contributions or encourage upvotes from a third-party site (Graham, Hacker News Guidelines). In addition to listings receiving upvotes, users may receive “karma” points. Contributors get karma points through contributing articles to the site that receive a high number of upvotes (Graham, Hacker News FAQ). The amount of karma points a user has can be viewed on their profile. Users who take actions which are undesirable on the site, such as engaging in fights in the comments of a listing, will be subjected to a downgrade in the number of karma points they possess (Graham, Hacker News FAQ).

The creator of the site, Paul Graham, has alluded that *Hacker News* is an experiment in preventing decline in quality of submissions a site receives. In a note to *Hacker News* users Graham stated that he “wanted to try to recreate the way Reddit felt back in 2006, when the users were mainly hackers. As Reddit became more popular, its focus inevitably changed. This was good for most users, but it left some of the earlier ones feeling left out. We wanted to create a new home for people like us," (Graham, 2007). By 2015, *Hacker News* was receiving 2.6 million views a day, 300,000 daily unique IP address visits, and 2-3.5 million monthly unique IP addresses (Rao, 2013).

The "Hacker Classics" List

The "Hacker Classics" list is a separate site from *Hacker News*, although it is also hosted by Y Combinator. Anything with more than 40 upvotes on the *Hacker News* site is included on the "Hacker Classics" list. The "Hacker Classics'" site description states that it "is no different from most of today's web in emphasizing what's new. When you're following a bunch of feeds, it's easy to forget that the web is the greatest library in the history of the world—and that a good library doesn't just have a rack of newspapers, it has a vast collection of books and archives: the stacks. Here, then, are the stories that occasionally surface on news.yc when someone goes diving into the stacks" (The Hacker Classics).

The "Hacker Classics" list is assembled by an algorithm which seeks to identify what people choose to view on the *Hacker News* site. There are 2,727 stories/news items on the "Hacker Classics" list, as of August 28th, 2018. The list is still being updated as listings continue to be contributed to and upvoted on the *Hacker News* site. Each listing must include the year which the content of the listing was originally published so that it can be properly added to the "Hacker Classics" list, which is organized in chronological order of the listings' creation. The "Hacker Classics" list includes entries from 1900 to 2010. Roughly half of the list comes from before

2004, meaning that a time period of six years, from 2004 to 2010, makes up the latter half of the list.

Reference:

The Hacker Classics. (n.d.). Retrieved from http://jsomers.net/hn/

James Sommers: Creator of the "Hacker Classics" List

The "Hacker Classics" List was created by James Sommers. Sommers is a writer and programmer based in New York (LinkedIn). He wrote the program for "Hacker Classics" on GitHub, a software development platform (The Hacker Classics). He has written for a number of publications and blogs (jsomers.net). He can best be described as having an organized, chronological mind, as exemplified by the organization of the "Hacker Classics" List, and a list of every book he has read since he entered college which is accessible on his personal webpage (jsomers.net). He is largely self-educated and has been trying to personally advance his own knowledge on a variety of subjects. He is a self-taught coder and shares his story of learning how to code in an article titled "How I Failed, Failed, and Finally Succeeded at Learning How to Code" which was published in *The Atlantic* magazine in 2011 (jsomers.net).

Sommers graduated from the University of Michigan in 2009 with a major in economics (LinkedIn). He has worked as a programmer for more than 10 years and was invited to write software during the Google Summer of Code in 2008. Sommers wrote the Google Chrome extension labeled as “Draftback” for Google Documents at the Center for Complex Systems. Draftback allows users to playback a visual depiction of edits made to a Google Document and is primarily used by educators to “play back” the revision history of the writing process among students. Currently, Sommers is working as a coding freelancer (LinkedIn).

Purpose

The purpose of this paper is to use the most upvoted material from the “Hacker Classics” list to reveal the historical awareness and characteristics of hackers, and thereby create a more holistic definition of what it means to be a hacker.

Hackers have a greater impact on the public than many realize, as they are responsible for many of the technological enhancements that people frequently take for granted. As with any influential person, it is interesting to know why and how they became what they are known as today and what control they have on the future.

Hackers are a segment of society that most of us feel removed from if we do not identify as members of the hacking community. We merely possess baseless assumptions about how they think, or operate, and so we find them to be mysterious. We create our perceptions of hackers through popular culture, like fictional movies and television, which does not always give an accurate portrayal of hacker or their work. As outsiders of the community we don’t clearly understand what motivates them. In order to attempt to understand the internal motivations of a hacker you must be a hacker yourself or become knowledgeable through research.

Hypothesis

Prior to beginning our research, we had many preconceived notions regarding the personas of hackers and the activities they engage in. We believed that there were common, specific characteristics that must be fulfilled in order for someone to possess the title of a "hacker." These beliefs that we held prior to engaging in research regarding what it means to be a hacker serve as our hypothesis of what the holistic definition of hacker was. The information detailed in this section serves to illustrate some of the most prominent views we had prior to our research and along with the identified themes from the "Hacker Classics" list, helped guide the topic areas of our secondary research.

We found it hard to define the term "hacker" because the definitions of professions and experts are constantly shifting. We primarily thought of "hacker" as a label one has in regard to their profession and abilities. We presumed that hackers have performance standards and an image they want to uphold. But we soon learned that their standards and image may vary from group to group and individual to individual within the hacking community. In general, we believed hackers take their profession as seriously as an accountant takes their professional occupation. Although some hackers may hack as a hobby, while others do it as an economic imperative. Now we are not so sure.

In popular media hackers are portrayed as possessing skills that are weird and unusual, but we quickly learned that these skills — which are described as abnormal — are actually becoming more highly in demand as technology continues to rapidly advance. We now realize that in the future the jobs people will be doing in any field relating to technology will incorporate skills that were once attributed solely to hackers. In other words, we predict that hacker culture will become more mainstream in the near future.

Another of our preconceived notions regarding hackers was that that they do not typically seek academic degrees, as they are not challenged by traditional education. We thought of them as being primarily self-taught and displaying mastery through practice and the repeated trial and error. We believed that hackers do not like power hierarchies or reporting to bosses or other professional authorities, as they are intrinsically motivated. They eschew traditional rewards, and don't need public recognition. Instead, they want their work to speak for itself. We also asserted that hackers do not like it when access to information is restricted, they prefer sharing and openness so that they can continue to advance their knowledge on a variety of topics.

Research Process

We began this project by analyzing the "Hacker Classics" list. We first broke the list into 6 sections based on the dates of the listings so that they were roughly equal in how many listings were contained in each of the categories. The six sections and the listings within them were divided into the following time periods; 1900-1980, 1981-1993, 1994-1999, 2000-2005, 2006-2008 and 2009-2010. We analyzed the listings in each of these sections, focusing on one section at a time, by reading the titles of each of the entries and skimming the contents of each listing to identify common themes (see Appendix). The themes identified included topics such as math, art, literature, space, programming languages, and video games. These themes were used to identify some of the interests and beliefs of hackers.

After identifying common themes of the listings, we compiled a list of significant historical events and technological advancements that occurred between 1900 and 2010, the time span of the list's entries. We compared the timing of these events with the themes we identified through analyzing the entries and noted any correlations. For example, we identified "space" as a prevalent theme in the category of listings from 1900-1980 which aligns with the historical event known as the space race which occurred between 1955 and 1975. By comparing important events to the themes, we identified from the listings we began to create a more complex understanding of the history of hacking. By basing our findings on a chronological history, both from the list and the historical events, we were able to pinpoint certain topics from the past that have interested hackers in recent times and could see the progression of these topics as technological advances were made.

The next step of our research was to address why these topics may have been of interest to hackers. We addressed this question by identifying areas for further research. These broad areas of research resulted in each of the parts of this paper; Hacking Defined, Psychology and Ideology [of hackers], and Groups and Communities [of hackers]. Through analyzing secondary research through the guiding lens of the themes/areas of interest identified in the "Hacker Classics" lists we were able to draw conclusions regarding what it means to be a hacker.

Part I: Hacking Defined

Definition of a Hacker

The N*ew Hacker's Dictionary* defines "hacker" as "a person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary…A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular" (Raymond, 1996, p. 233). One way to visualize this definition is to think of computers as an iceberg. The tip of the iceberg is what the vast majority of people use computers for, typically simple, common tasks. The rest of the iceberg, which is not visible from the surface, is what hackers use computers for.

Blackies' Dictionary of Computer Science defines a hacker as someone "who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming," and someone "who enjoys the intellectual challenge of creatively overcoming or circumventing limitations" (Blackie's, 2013, p. 103). Hackers enjoy the action of going into computers and gaining knowledge about their intricacies. They are about action and not theorizing. Of course, hackers must have a plan before hacking, but it is the action of hacking that is most exciting for them and keeps them coming back for more. The key here is that in order for someone to be a hacker they cannot be merely thinking about hacking they must actually be taking actions whatever they may be.

History of the Term 'Hacking'

The Massachusetts Institute of Technology (MIT) is believed to be the birthplace of the term "hacking," as it has been traced back to being used on the campus as early as the mid-1950's (Ward, 2011). The first documented use of the word as it is defined today appears in the meeting minutes of MIT's Tech Model Railroad Club in the April of 1955 (CyberSecurity). The club used "hacking" to describe the modifications they made to the functions of their high-tech train sets (Power, 2016). Initially, the term "hacker" was not exclusively used to describe those altering the technology, it simply described individuals that had a desire to take things apart and "make them work slightly differently than intended" (CyberSecurity). Many of the earliest hacks were intended to entertain, not cause harm, such as a hack MIT students pulled on the Harvard-Yale football game in 1982, when they released a growing black balloon onto the field which exploded in a cloud of white vapor (CyberSecurity).

The 1970's saw the rise of telephone hackers, also referred to as "phreakers" (Power, 2016). As the telephone switching network went completely electronic, individuals began tampering with the network. One of the most infamous phone hackers, John Draper, discovered that a whistle distributed as a prize in Cap n' Crunch cereal boxes produced the same tone used to indicate that a telephone line was available to route a new call (Power, 2016). Draper and other phreakers began using the whistle to make free long distance calls (Power, 2016).

The term “hacker” was re-appropriated during the 1980’s and 1990’s, as the computer industry rapidly expanded and individuals could more easily acquire computers for their personal use (CyberSecurity). As individuals who identified themselves as hackers began getting caught tampering with computers, a negative connotation was firmly attached to the term. Prosecutors of these crimes and the press covering them began using the term to describe individuals who broke any law through the means of a computer (CyberSecurity). The emergence of cyber criminals and computer viruses prompted the creation of the Federal Computer Fraud and Abuse Act created in 1986 (Power, 2016). As technology continues to evolve the definition of the term will likely continue to change alongside these advances.

Part II: Psychology and Ideology

Psychology and Shared Traits of Hackers

By analyzing listings from the “Hacker Classics” list that contained the words “hack,” “hacker,” or “hackers” a greater understanding regarding the psychology and shared traits of hackers was reached. One commonality of hackers is that they like to be intellectually challenged and hate being bored. One of their primary beliefs is that “the world is full of fascinating problems waiting to be solved” (How to Become a Hacker, 2001). Despite it being clear that hackers are intelligent, they don’t necessarily excel in school. As portrayed in “The Conscience of a Hacker”

(1986), individuals may feel that they are smarter than the other kids and that what they are learning in school bores them as they are so ahead of the group that they feel restricted. The feelings conveyed in passages such as “you bet your ass we’re all alike... we’ve been spoon-fed baby food at school when we hungered for steak...” reinforce the idea that hackers want to be challenged and move on to new endeavors once they have grasped a concept fully (The Conscience of a Hacker, 1986). The work “What is a Hacker?” (1985) goes so far as to say that a hacker is “someone who never goes to class, who in fact sleeps all day, and who spends the night pursuing recreational activities rather than studying.” This notion is reinforced by passages from “The Hacker Papers” (1980) which state that “what occurs is that the hacker’s motivation to challenge themselves in any field not directly linked to computers gradually disintegrates. On the level of grades, straight-A students tacitly accept C's in non-computer courses.”

Another shared value of hackers is that they are not motivated by money or recognition. Rather, they simply want to embark upon new challenges and innovative ways of problem solving. The publication “What is a Hacker” asserts that “computer programming must be a hobby, something done for fun, not out of a sense of duty or for the money. (It is okay to make money, but that cannot be the reason for hacking).” This statement is validated in “The Jargon File,” which states that “hackers are generally only very weakly motivated by conventional rewards such as social approval or money” and the idea perpetuated in “Great Hackers” (2004) that “ordinary programmers write code to pay the bills. Great hackers think of it as something they do for fun, and which they are delighted to find people will pay them for.” This outlook coincides with the shared attitude noted in “How to Become a Hacker” (2001) that “boredom and drudgery are evil.” Hackers simply want interesting projects that will allow them to discover a new solution

(Great Hackers, 2004). As “Legendary Hackers” (2010) notes, hackers can be classified as people “who enjoy the intellectual challenge of creatively overcoming or circumventing limitations." This shared need to exercise their knowledge and skills through difficult problem solving is a clear commonality among hackers.

“The Hacker Papers” (1980) more positively describes hackers as “self-contained,” explaining that “their entire social existence usually centers around one another...Very, very few associate much with anyone who is not at least partially a member of the hacking group.” Although many hackers may have felt socially isolated prior to hacking they may become even further removed from social groups as they believe “being something of a social outcast helps you stay concentrated on the really important things, like thinking and hacking” (How to Become a Hacker, 2001). Their infatuation with computers takes up their free time and they can even form an incredibly close and dependent relationship with technology. In “The Conscience of a Hacker” (1986) it is clearly described how computers afford the hacker a way to fill the void of social isolation and a degree of accountability that can be traced to their actions that they have never experienced before as the author recounts “I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me...” Over time “the personality of the hacker shifts, in order to permanently adjust to the new social conditions. Emotions always hurt before so they are effectively isolated” (The Hacker Papers, 1980).

Study Relating the Psychology of Hackers to Their Success

Today, the term “hacker” has a largely negative connotation, as they are often portrayed in popular culture as conniving and taking illegal actions. There is still a great deal of interest in understanding what motivates a person to become a hacker. In a 2010 study titled “The Risk Propensity and Rationality of Computer Hackers” researcher Michael Bachmann defines hacking as “the act of re-designing the configuration of hardware or software systems to alter their intended function” (Bachmann, 2010, p. 643). Bachmann’s study proposes that there are two personality characteristics commonly ascribed to hackers: strong preference for rational decision-making processes and pronounced risk propensity (Bachmann, 2010, p. 643). The study focuses on examining these two personality characteristics and their effect on hacker’s activities, motivations, and successes.

Bachmann’s study involved distributing a survey to measure the extent to which hackers practiced analytical-rational or intuitive-experiential information processing and risk propensity (Bachmann, 2010, p. 646). The sample included 124 hackers who were attendees at the 2008 ShmooCon hacker convention, one of the “largest and most popular annual conventions worldwide” that takes place in Washington D.C. (Bachmann, 2010, p. 644). The purpose of the survey was to see if there was a relationship between hackers who have a strong preference for rational decision-making processes and pronounced propensity with their involvement and success in hacking-related endeavors. This was evaluated by comparing the survey responses from hackers to those of the general public (Bachmann, 2010, p. 643).

The survey results indicated that hackers do have a “considerably higher need for cognition and higher risk propensity than the general public” (Bachmann, 2010, p. 652). Both personality characteristics of preference for rational-decision making processes and risk propensity were found to be statistically significant in predicting hacker related outcomes (Bachmann, 2010, p. 652). The results also displayed a positive correlation between risk propensity and number of total hacking attempts (Bachmann, 2010, p. 650). However, hackers with a high preference for rational-decision making were more confident in their abilities and thus more successful in their hacking attempts than those who had a less pronounced preference for rational decision processes, who were less confident in their abilities (Bachmann, 2010, p. 652). The study also found that hackers with a stronger risk propensity initiated more hacking attempts, but had less overall success than those who did not have a strong risk propensity (Bachmann, 2010, p. 652).

In addition to the survey findings, Bachmann also asserts that to be a successful hacker one must possess both the knowledge necessary to understand how a piece of technology functions and a degree of creativity that allows the hacker to envision the changes to the technology (Bachmann, 2010, p. 643). Although the term “hacker” is used to describe a large range of people in regard to their knowledge of computers and their motivations, Bachmann states that the connection between all people given the label of “hacker” is that they are both knowledgeable and creative when it comes to altering technology (Bachmann, 2010, p. 643).

Reference:

Bachmann, M. (2010). The Risk Propensity and Rationality of Computer Hackers. *International*

Journal of Cyber Criminology, 4(1&2), 643–656. Retrieved from https://pdfs.semanticscholar.org/bf09/3c90e7cba8c50b1244db02902973f3f5d896.pdf

Political Views

The political views of hackers range across the entire spectrum. However, many do identify as libertarian, as they reject the conventional bipartisan structure of politics completely. For this reason, hackers tend not to be found on either of the extreme ends of the political spectrum. Some hackers reject conventional politics and present themselves as apolitical because they do not want to ascribe to any one label.

One commonality amongst hackers is that they are generally anti-authoritarian. They value individual thought and are more interested in personal belief systems than organized political systems. Hackers tend to be very committed to their beliefs and can provide evidence and reasoning as to why their beliefs are superior. One political area of interest to hackers is the protection of free speech. Many hackers argue that the act of hacking is protected under free speech laws. This opinion is largely controversial outside the hacking community, as many believe that hackers stretch free speech laws too far in order to justify the legality of their actions.

Election hacking is gaining more recognition from the media in recent years. Many instances of election hacking do not appear to benefit or harm one political parties, instead both parties have been positively and negatively affected. There is no clear correlation between the intended outcomes of all instances of election hacking as different hacking groups are responsible for different occurrences of it. The only commonality is that election hacking disrupts the system established by governments for voting procedures and declaring election results. Some hackers may just be pleased with their ability to disrupt such a large, seemingly protected system, as it provides them with a challenge and a great sense of power if they are successful.

Reference:

Raymond, E. (n.d.). Politics: Appendix B. A Portrait of J. Random Hacker. *The Jargon File (version 4.4.7)*. Retrieved from http://catb.org/jargon/html/politics.html

Female Hackers

Hacking, like many other technical fields of work, is a male dominated profession. However, there are known female hackers. Many hackers have stated that they do not believe that females are treated inferior to male hackers. They assert that rather than gender, a hacker's skill level determines their worth in the eyes of their fellow hackers. This may in part be due to the fact that many hackers use usernames which disguise their gender so that it does not play a role in other hackers' preconceived perceptions of their abilities (Raymond, Gender).

It has been noted that the type of hacking that females are involved with generally varies from males. Most female hackers do not seem to be engaged in criminal activity. Many females who identify as hackers may be consultants on cybersecurity or professors in computer science or other related fields, with extended knowledge of hacking. Generally, female hackers are thought to predominantly engage in "socially approved" hacking (Raymond, Gender).

One example of a female hacker utilizing her skills to benefit others is Suz Hinton. By day, Suz works as a Cloud Developer Advocate at Microsoft, meaning that she partners with companies and communities to assist them with utilizing Azure Cloud Services and other Microsoft tools. By night, Suz builds JavaScript hardware libraries for others to utilize and streams as she lives codes on the streaming platform Twitch, so others can tune in to see her display her skills. Suz learned to code when she was just nine years old and has continued to update her skills as new programming languages and technology continue to be developed. When asked what her favorite part about coding is, Suz replied that it is her ability to "help others with my coding skills. If I see a service or tool that doesn't exist, I have the ability to create it to hopefully improve my life or others' lives." This desire to help others is evident in Suz's creation of the Personal Ultimate Reassurance Response (P.U.R.R.) Bracelet, which Suz created during a hackathon to help those suffering from anxiety, as it measures heart rate and when it senses an escalation in the wearer's heart beats per minute, it will text them a cat photo to cheer them up. Suz is just one example of a female hacker who has gained recognition for her notable accomplishments and approach to hacking (Chen).

Though the computer science fields are historically male-dominated, there are increasing efforts to support and encourage women in technical aspects of computing. One such organization that is working towards increasing the population of female computer scientists is Systers. Systers "provides a private, safe online forum for women involved in technical aspects of computing. Our members gain support by networking, sharing advice and experiences, and collaborating on various projects." (Systers) The online Systers forum was started by Anita Borg, a female computer scientist with a Ph. D. from the Courant Institute at New York University and the founder of the Institute for Women and Technology, who made it her mission to "increase the number of women in computer science and make the environments in which women work more conducive to their continued participation in the field." Since it was founded in 1987, Systers has become the largest email community of women in technical commuting, currently engaging over 7,500 members from more than 65 different countries. (Systers)

Though Systers, and other similar organizations and communities are attempting to break down the stereotype that hacking, information technology, and computer science are 'male' professions, women in these fields tend to be highly underrepresented.

Differences Between Black, White, and Grey Hats

Although hackers are stereotyped as all having evil, destructive goals to gather protected information, there is actually a wide range in the intentions of hackers. A common way in which hackers are distinguished based on their goals is by labeling them as a "white hat," "grey hat," or “black hat.” The color of hat a hacker dons is based on two main factors; “their motivations, and whether or not they are breaking the law.”

Black hat hackers are those who are commonly thought of when the word hacker is used because of the way hackers are portrayed in pop culture. They are often motivated by personal or financial gain or and will break laws in order to succeed in their hacking attempts. They are the hackers who write and initiate malware on others’ computers and often seek to gain sensitive data in order to alter or distribute it.

White hats are the opposite of black hats, they are the good guys and act ethically. They are often employed by government entities to find flaws in security that black hats can exploit. The primary difference between white hats and black hats is that white hats generally only act if they have permission from the system’s owners, while black hats act entirely without permission and their goal is to not get caught.

Grey hats are the median between black and white hats. They can either have ethical or financial motivations. Often, they may hack into a system without permission, but will alert the owner if vulnerabilities are found so that they can be changed to produce greater protection. The label of grey hats is also used when the motivations or legality of a hacker’s actions are unclear or cannot be easily categorized.

Hacker Rich Christie attributes the variation in hacker types to their motivations. He summarizes his argument by asserting that unethical, black hat hackers will be motivated by “greed, hate, bias, and a destructive mindset,” while ethical, white hat hackers may be motivated by “an intellectual challenge, innovative ingenuity, and the like.” Christie states that “the line between ethical and unethical hacking is a thin one,” partially determined by the hackers themselves, as well as the opportunities presented to them based on their skills and abilities. The jobs hackers choose to accept or create for themselves are reflective of their motivations, and therefore indicate what type of hacker they are (WebExpert, 2009).

Study on the Psychology of Black, White, and Grey Hats

Despite hackers being stereotyped by the media as awkward, nerdy, antisocial young men, they can be quite diverse in terms of their personalities. The motives of today’s hackers and extent of how ethical their actions are can also vary greatly. By examining the various subgroups of hackers based on their motives and ethical standards, specific conclusions about their personality types can more accurately be made.

A 2016 study conducted by Andik Matulessy and Nabilla H. Humaira, titled “Hacker Personality Profiles Reviewed in Terms of the Big Five Personality Traits,” examined the personality types of three hacker groups; the white hats who hack in an ethical manner, grey hats whose motives are often unclear, and black hats who hack for personal gain and are driven by unethical motives. The study utilized the “big five personality traits,” which include openness to experience, conscientiousness, extraversion, agreeableness and neuroticism, as a method of categorizing the hackers' personalities. The study had thirty participants whom the researchers conducted interviews with, administered rating scales to, and administered other qualitative methods to determine the participants' dominant personality trait out of the "big five personality traits" examined.

The study concluded that white hats demonstrate agreeableness as a dominant personality trait, while black hats demonstrate openness to experience, or the willingness to partake in unfamiliar things, as their domain personality trait. Neuroticism, defined as the "opposite of emotional stability," which can include feelings such as anxiety and sadness, was found to be the primary trait demonstrated by grey hats. These findings point to clear distinctions between the personalities of the various hacker types.

Reference:

Matulessy, A., Humaira, N. H. (2016). Hacker Personality Profiles Reviewed in Terms of the Big Five Personality Traits. *Psychology and Behavioral Sciences*, *5*(6), 137-142. Retrieved from http://article.sciencepublishinggroup.com/html/ 10.11648 .j.pbs.20160506.12.html

An Interview with a Black Hat

In *Freedom from Fear* Magazine's 7th edition, Raoul Chelsea, in coordination with the UNICRI Management and External Relations team, interviewed an anonymous black hat hacker. The hacker discussed that they identify as a black hat because hacking is their job and it earns them a salary. They stated that they run black-ops for their employers and that they charge a high fee for their services. They discussed their introduction to the hacking community, and how their friends already in the community and their own abundance of free time allowed them to learn about what hackers around them were doing. The black hat stated that at first their involvement in hacking was just for fun, "hacking into servers, stealing information, pictures… a lot of fun," but things got more serious when payment started being offered for their services.

The black hat also stated that the nature of their work has changed over time. At the beginning their motivations were curiosity and learning, but that changed when money became a factor. For the black hat, money became involved when they realized that they could provide a service and that others could not provide or didn't have the skills to perform. They realized that they could capitalize on these learned skills and use them to make a profit. At first, they worked in a group with others, but over time people came and went from the group. Each of the new group members brought varying levels of experience and knowledge with them, but as these people moved on from the group, the black hat stayed and learned. Today the black hat has accumulated enough knowledge to work alone, but occasionally buys information and help from friends and other hackers.

The interviewed hacker self-identifies as a black hat not only because they receive payment for their work, but also because the nature of the work they have done. In response to a question about their past criminal activity the hacker replied, “I guess [that] would include gaining unauthorized access to computer systems and networks; stealing accounts, personal information, and selling them out. And I guess also industrial espionage and money laundering.”. They acknowledged that their line of work comes with the consequences tied to cybercrime laws, but they admitted that these ramifications were not a deterrent to their activities. In their mind, the potential consequences and difficulties that come with the job are what makes it more interesting and fun. They view every job is a challenge, and when a job stumps them they simply must think of another way to attack the problem.

This black hat noted that although they enjoy the work that they do, they aspire to “stop working in 2 or 3 years,” retire, give money back to their family, and buy their own house. Like others whose work is doing something they love, for this black hat hacking is just a hobby that turned into a lucrative occupation.

Reference:

Chiesa, R. (2010, July). Interview with a Hacker: Chronicles of a Black Hat. *Freedom from Fear, 7,* 5. Retrieved from http://f3magazine.unicri.it/?p=333

The Hacker Ethic

“Hacker ethic” is a term used to describe the unique work ethic that all hackers are generalized to possess based on interviews and the experiences by famous hackers. This work ethic is fueled by a hacker’s intrinsic motivations and pure enjoyment of the acts of programming and hacking. The problem-solving nature of hacking has been noted as a key reason why the act appeals to hackers. Their genuine curiosity and eagerness to find new solutions to existing problems, as well as their desire learn about how things work, pushes hackers to get up and work for hours and hours each day. An example of this “hacker ethic” is “the way sixteen-year-old Irish hacker Sarah Flannery describes her work on the so-called Cayley-Purser encryption algorithm: ‘I had a great feeling of excitement. . . worked constantly for whole days on end, and it was exhilarating. There were times when I never wanted to stop’” (Himanen 2001).

The “hacker ethic” is also fueled by the joy of hacking. Apple co-founder Steve Woznick has said that many of the characteristics of the first Apple computer came from a game that he was creating just for pleasure, to show off to other programmers. To quote Eric Raymond, a well-known defender of hacker culture, “software design and implementation should be a joyous art, and a kind of high-level play. If this attitude seems preposterous or vaguely embarrassing to you, stop and think; ask yourself what you've forgotten. Why do you design software instead of doing something else to make money or pass the time? You must have thought software was worthy of your passions once. . . To do the Unix philosophy right, you need to have (or recover) that attitude. You need to care. You need to play. You need to be willing to explore.” (Himanen 2001) This passion and desire for exploration is what motivates hackers to continue to work, program, and problem solve. This type of motivation is what most people look for in their future careers, but for hackers this work ethic comes naturally because they are not bound by bosses and restrictive timelines. The autonomous nature of a hacking career allows for programmers to work on their own time, explore what they want to, and work on things they enjoy.

To summarize the idea of the “hacker ethic” it is best to look at the work and passion that Linus Torvalds exemplified in his Prologue. For the hacker, "the computer itself is entertainment, meaning that the hacker programs because he finds programming intrinsically interesting, exciting, and joyous.” This type of work ethic is not restricted to hackers, but it has been observed that it is organically found in hackers. It has been said that if one can take this type of work ethic and apply it to any of their interests they can make a career out of any hobby or passion that they wish to dive into.

Reference:

Himanen, P. (2001). The Hacker Work Ethic. In *The Hacker Ethic and the Spirit of the Information Age.* New York, NY: Random House. Retrieved from https://archive.nytimes.com/www.nytimes.com/books/first/h/himanen-hacker.html

Part III: Individual Hackers

We researched the biographies of some noteworthy individual hackers to form a clearer understanding of the backgrounds and accomplishments of some hackers. The following sections are detailed descriptions of accomplished hackers, their work, accomplishments, and motivations. We analyzed the individuals' stories and looked for similarities between them in order to determine if there were specific characteristics amongst these individuals, who despite being from many different in many aspects, share the commonality of possessing the title of "hacker."

Paul Graham and Robert Morris: Founders of Y Combinator

Paul Graham is a computer scientist, entrepreneur, venture capitalist, author, and essayist. He received a Bachelor of Arts in Philosophy from Cornell and both a Master of Science and Doctorate of Psychology in Computer Science from Harvard (People). Graham is the author of numerous books relating to programming, including *On Lisp*, *ANSI Common Lisp*, and *Hackers & Painters* (Bio). Graham has also gained recognition for many of the essays published to his personal site, paulgraham.com (Bio). In 1995 Graham and Robert Morris started Viaweb, the first software as a service company, which was then acquired by Yahoo in 1998 (People). Graham, along with Morris, Jessica Livingston, and Trevor Blackwell were the founders of Y Combinator. When asked why Graham and his colleagues started Y Combinator, Graham explained that "the real reason we started Y Combinator is one probably only a hacker would understand. We did it because it seems such a great hack. There are thousands of smart people who could start companies and don't, and with a relatively small amount of force applied at just the right place, we can spring on the world a stream of new startups that might otherwise not have existed," (Graham, Why YC). *Hacker News* is the brainchild of Graham, who started the site while he was working at Y Combinator (Graham, What I've Learned). Graham left Y Combinator in 2014 (People).

In 1999 Robert Morris, a student at Cornell, created one of the first computer worms (Lee, 2013). The "Morris Worm" infected every computer that it came in to contact with. It passed from computer to computer by way of email and unprotected user logins. The worm was not malicious, in that it did not actually steal information from the computers, it simply exploited a common hole in system securities by slowing them significantly or causing them to cease to function (Kelty). It would take up to two days to get the virus off an infected computer, resulting in some regional computers being forced to disconnect from the backbone network so that they could be cleaned up (Lee, 2013). Morris' worm is thought to have infected 10 percent of all computers attached to the internet at the time, resulting in about 6,000 computers being compromised (Bortnik, 2013). Morris was the first person sentenced under the Computer Fraud and Abuse Act (Kelty). After serving out his sentence, he became a college professor and later became a co-founder of Y Combinator (People).

Kevin Mitnick

Kevin Mitnick, once deemed the "world's most wanted hackers" by publications like Wired and Forbes, has turned in his black hat and now dons a grey one. Mitnick's hacks began before the age of 18, with acts such as tampering with the Los Angeles Bus system's punch cards so that he could ride for free and taking over the drive-through speaker at his local McDonald's. As Mitnick grew older his hacks grew much more sophisticated, and more criminal. In 1995 Mitnick was caught by the FBI and sentenced to five years in prison after he “skillfully eluded and bypassed corporate security safeguards, penetrating some of the most well-guarded systems, including, amongst countless others, the likes of Sun Microsystems, Digital Equipment Corporation, Motorola, Netcom, and Nokia” (Coleman). In total, Mitnick was charged with 14 counts of wire fraud, 8 counts of possession of unauthorized devices, interception of wire or electronic communications, unauthorized access to federal computer, and causing damage to a computer (Coleman). His arrest and sentence was incredibly controversial, as many members of the hacking community argued that Mitnick’s sentence was far too long, given the crimes he committed and his supporters even created “Free Kevin” shirts and stickers (Greenberg).

Today, Mitnick has shifted from the illegal acts of a black hat, to those of a grey hat. One of Mitnick’s first business venture after prison was the creation of Mitnick Security, which provides penetration testing and security consulting for businesses. More recently, Mitnick has developed a new branch of his security consultancy business, called Mitnick's Absolute Zero Day Exploit Exchange (Greenberg). The Absolute Zero Day Exploit Exchange offers “to sell corporate and government clients high-end ‘zero-day’ exploits, hacking tools that take advantage of secret bugs in software for which no patch yet exists” (Greenberg). The sale of potential surveillance tools through this process by hackers has been met with widespread criticism from those concerned about both the ethical implications of these sales and the security threats they may lead to (Greenberg). Kevin’s widely known criminal past makes his involvement with this type of service even more controversial, as he has displayed that his means of achieving his goals and earning an income are not always legal (Greenberg). Mitnick continues to be one of the most notable individuals in the hacking community, as media outlets continue to cover his most recent developments and achievements relating to Micnick Security.

Andrew Horner

When you think about job applications what comes to mind? Countless hours spent trying to perfect your resume? Writing what seems like at times hundreds of personalized cover letters for each individual application? The "reverse job application." takes a completely different approach.

The creator's name is Andrew Horner, and he takes users through three stages of his life; the past, present, and future. Two years out of college and Mr. Horner was still jobless. He was wondering why no employer would give him a chance. It wasn't like he was a deadbeat. In fact, he was the complete opposite; he was at times overqualified for the jobs he was applying to, and yet did not hear back from any companies. Reflecting on how he felt at the time he wrote "the flickering flame of a candle in a tempest of uncaring and unforgiving societal expectations." He goes on to say that he was beginning to feel like college was a complete waste of time and the countless hours he spent studying in the library were going to waste. His worst fears were actually unfolding before him (Andrew Horner).

Horner was waiting in line at a McDonald's drive thru when he had an epiphany. Fast forward to the present and explains his idea of a reverse job application, which served the opposite function of a normal job application. Instead of sending in his resume and cover letters, Horner developed a website where employers could actually apply for him to come work for them. He believed that having people apply to him would allow him to make contact with more employers, and therefore have more choices and opportunities. He developed a set of credentials that he would require in a future employer, and provided a list of qualities that he would bring to the workplace. If a company did not match his needs for an employer he encouraged them "to liberally institute company-wide changes" until they did (Andrew Horner).

A note on the site states that Horner's creation of the did result in him landing a job after many years of traditional job searching. Horner's reverse job application has been criticized for being a way in which Horner displays his arrogance. His response to critics is that "the obvious arrogance in the reverse job application is a result of the narrative voice I decided to use, rather than a reflection of my day-to-day personality." On the other end of responses, when praised for his innovative idea he counters saying that "I'm just a guy who did something goofy as a way of turning the tables on a system that hadn't been working for him." This way of thinking is the epitome of what hackers try to do, find creative solutions to problems (Amazing).

Bill Gates

Bill Gates is someone who consistently appears throughout the articles in the "Hacker Classics" collection. This is of no surprise considering he is one of the most influential people in the 21st century in many regards, in part due to his development of software through his company Microsoft. Bill Gates' notable history of technological accomplishments began in a dorm room at the Harvard University. Bill’s roommate, Paul Allen, proclaimed “hey, this thing is happening without us,” and proceeded to hand him the January 1975 *Popular Electronics* magazine about the latest technology. Bill read the article and agreed with Paul that he was right. The two of them spent the next eight weeks frantically writing code. The end result was something profoundly impactful on the future of the computer business, the invention of Microsoft.

Gates was first introduced to a computer terminal while attending Lakeside, a private middle and high school. In eighth grade Bill, Paul, and several others formed the Lakeside programming group. The group taught themselves BASIC and were soon able to master other, more challenging programming languages, such as COBOL and Fortran. Gates had the unique ability to focus on one task at a time with complete focus. These relatively humble beginnings are something that many hackers can relate to and admire. Bill’s ability to transform himself into one of the richest and most influential people in the 21st century through the development of software is an aspiration of many hackers.

Bill Gates associated himself with like-minded individuals, and from a very young age was able to recognize potential in these people. He sought to advance not only himself, but wanted to help the world change. Looking at Bill Gates’ early beginnings gives a good perspective of how hackers come to be. As evidenced by the few situations described above, from a very young age, Bill Gates was driven to be the best hacker there ever was.

Reference:

Encyclopedia Britannica. (2019, March 8). Bill Gates: American Computer Programmer, Businessman, and Philanthropist. *Encyclopedia Britannica.* Retrieved from https://www.britannica.com/biography/Bill-Gates

We found that there is little that distinguishes the "extraordinary" hackers from the "average" hackers. Despite the prominence of Bill Gates' name his primary motivation for his hacking, curiosity, and desire to produce innovative work is similar to that of lesser known hackers, such as Paul Graham and Robert Morris. While the stories and goals of each of these hackers vary, it is evident that they all seek to fill a gap in a service that can make life easier or solve a problem that they view as worthy of dedicating time and effort to.

Part IV: Groups and Communities

Hacker Groups

Hacker groups are a physical representation of the Social Banditry Theory, which explains that people who tend to feel "voiceless" band together for support and act as disruptors of the world that they are unsatisfied with (Sloat, 2017). These groups tend to be composed of people who see the world in a collective way, where everyone is working together and contributes to the well-being of society. Due to this outlook, they see their role as hackers as an important method of restoring justice in a way that takes power away from those who they believe are harming the collective whole of society. Hacker groups come together to share skills and expertise in order to make a changing impact through hacking and cyberattacks/cybersecurity. In their eyes, they are doing necessary work that is essential in preserving or changing the system that they see as being flawed. (Sloat, 2017)

Below are descriptions of two hacker groups and the kinds of activities that they engage in. These hacker groups are examples of typical hacker groups and the ideologies that they seek to uphold.

Anonymous is a decentralized hacktivist community, with members all around the world. They have launched several attacks on various countries, political, and religious groups. They are not affiliated directly with WikiLeaks but they are very supportive of that other group. One of their attacks was on the Church of Scientology. They chose to hack into the Scientology mainframe in order to try to disrupt the church. The reason for this was because the church got YouTube to take down a video of an interview with one of their key members Tom Cruise. They viewed this as a violation of freedom of speech which is one of their core ideals.

LulzSec is loosely affiliated with Anonymous and they are known for their attacks on compromised security systems and bringing attention to the dangers of password reuse. Their main motivation is to have fun and do it for the “lulz,” as they are a not-for-profit group. (Taylor 2011) Different than most other hacker groups, Lulzsec is known for releasing the names and information about the people and companies that were hacked in order to bring attention to the importance of cybersecurity and essentially ‘require’ such entities to employ stricter protection methods. Recently, this group’s attacks have become more political in nature, as they have been focused on uncovering the corrupt and racist nature of the US government, military, and law enforcement agencies. Though not all hackers are involved in a group, the group dynamic that is apparent in hacker culture is important to recognize.

Reference:

Raza, A. (2016, January 21). 10 Most Notorious Hacking Groups. *Hack Read.* Retrieved from https://www.hackread.com/10-most-notorious-hacking-groups/

The Economics of Hacking

For a large amount of today’s aspiring hackers, the motivation to enter the competitive landscape of cybercrime is money. But the payouts for hackers varies significantly because of various factors including competition, the significance of the hack, what information the hack will supply to the client, and how much time and work the hack takes to complete.

Although black hat hackers may be compensated for a client for performing illegal acts to obtain desired information, there are becoming more ways for hackers to get compensated legally for their actions. For “white hat” hackers or “security researchers” there are jobs such as penetration testing and bug bounty programs, where companies hire hackers to attack their own products with the aim of uncovering problems that the developers can then fix. Companies either hire a specific hacker to do these jobs, or they release an offer to independent hackers and compensate them based on the type and magnitude of the flaws they find. These compensations can run upwards of $10,000 for individual bug finds and up to $100,000 for the discovery of previously unknown techniques that may require developmental changes in their products or systems (Peterson 2015).

As the market for hackers has rapidly expanded since the early 2000's websites and job boards like HackerOne and Bugcrowd have popped up, providing a forum for those seeking hackers to perform bug bounty programs and penetration testing (Peterson 2015). Even though these job boards and contests are becoming more commonplace, there are some companies that do not have bounty programs to pay off "researchers" because they feel threatened by an outside individual attempting to find flaws and gain access to the back end of their systems. However, most hackers tend to operate not as independent researchers, but in a sort of "gang" format, where groups of hackers work together to provide subscription-like support services to companies who are interested in finding flaws and existing bugs. As technology continues to change and advance there are becoming opportunities for hackers to use their knowledge and skills to earn a living.

Reference:

Peterson, A. (2015, November 5). Inside the Economics of Hacking. The Washington Post.

Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2015/11/05/inside-the-economics-of-hacking/?utm_term=.ab43161782da

Part V: Limitations

Due to the nature of the “Hacker Classics” list, this study is limited in scope and many pertinent topics remain unaddressed by the previously presented writing. These limitations stem from the fact that the “Hacker Classics” list is still live and being updated, therefore, it is always changing and the conclusions one can draw from the list are based on the contents of the list at the time of its viewing.

Also, the “Hacker Classics” list is limited in its publishing period; Though the list is still live and being updated, content referenced on the list is restricted to items with publication dates between the years 1889 and 2011. Therefore, there is a defined wall on what can be included on the list, excluding newer phenomenon, discoveries, technological developments, etc.. Consequently, there may be important elements of the hacker identity and areas for further research and analysis that may not be available on the list at all and were in turn not included in this study.

Additionally, due the fact that the list is generated based on a system of upvotes and because it is updated regularly, the conclusions drawn by this study are inferred based on what was found by looking back on the list. Which in turn means that the conclusions inferred by the list have the potential to be based on the popularity of the list, who actually knows about it, who is upvoting and can sway/ influence what types of content appear on the list. Unfortunately, this means that

that the list may not necessarily reflect the hacker community as a whole but a portion/ subset of the community. These subsets/ period of interest can be influenced by historical events that were influential at the time, and may lead to an overview of a hacker that is only a reflection of certain aspects/interests of hackers.

Due to the length of the list and the variety in content, narrow topics have gone un-analyzed in this study. Topics such as: mental health, drugs, war and army studies, toys, space, languages, the works of well-known individuals, natural and man-made disasters, mathematics, management and leadership, and others were not included in this study but are another area for further research and analysis in the future.

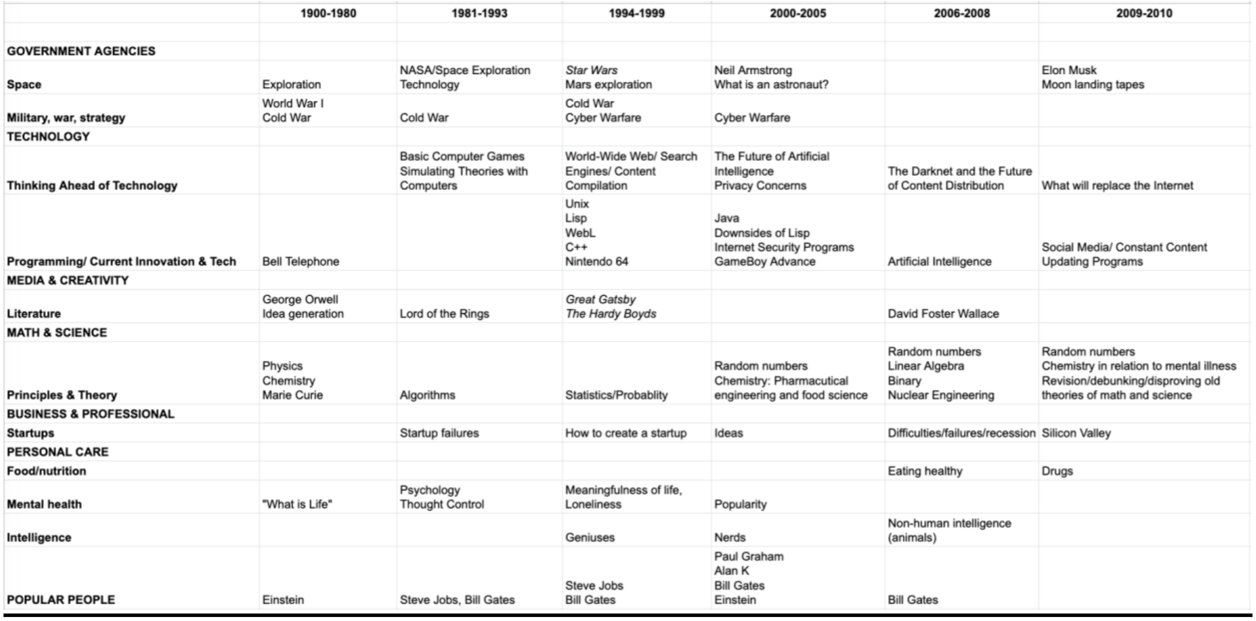
Conclusion

As a group, we started out with access to a single website which sparked our interest. The Hackers Classics contains a vast amount of information that we sifted through. We did not read every single article in the "Hacker Classics" with a fine-tooth comb, however we did try to obtain a perspective on what James Sommers was trying to accomplish in creating a site where content of interest was presented in a such a manner. We started out this project with a very shaky understanding of what a hacker is. We weren't sure about many of the intricacies of the field, such as the difference between a white hat and black hat, or the ways that hackers can legally make an income. By analyzing the listing of the "Hacker Classics" and then using our findings to guide the secondary research we compiled on hackers and their motivations we learned that there is not a single, all-encompassing definition of a hacker.

The definition of a hacker changes as time and technology does. This is something that the "Hacker Classics" makes very clear. In the early years when phones were first invented hackers were considered to be people who would tamper with the technology in order to make free phone calls. Then at the start of computer hacking hackers were programmers and coders. Now with the omnipresence of computers and the ever-changing world of technology, a hacker can take many different meanings.

We cannot predict what a hacker will be defined as in the future because we don't know what technological advancements there will be. However, through analyzing the classics and secondary research we can definitively state that a hacker is a knowledge seeker. This aspect of the definition of a hacker has remained the same throughout all the advancements in technology. Regardless of the technology tampered with or motivations of the individual, a hacker is someone who seeks to problem solve, and obtain both tangible and intangible things in order to accomplish their goals.

Appendix



	1900-1980	1981-1993	1994-1999	2000-2005	2006-2008	2009-2010
GOVERNMENT AGENCIES						
Space	Exploration	NASA/Space Exploration Technology	*Star Wars* Mars exploration	Neil Armstrong What is an astronaut?		Elon Musk Moon landing tapes
Military, war, strategy	World War I Cold War	Cold War	Cold War Cyber Warfare	Cyber Warfare		
TECHNOLOGY						
Thinking Ahead of Technology		Basic Computer Games Simulating Theories with Computers	World-Wide Web/ Search Engines/ Content Compilation	The Future of Artificial Intelligence Privacy Concerns	The Darknet and the Future of Content Distribution	What will replace the Internet
Programming/ Current Innovation & Tech	Bell Telephone		Unix Lisp WebL C++ Nintendo 64	Java Downsides of Lisp Internet Security Programs GameBoy Advance	Artificial Intelligence	Social Media/ Constant Content Updating Programs
MEDIA & CREATIVITY						
Literature	George Orwell Idea generation	Lord of the Rings	*Great Gatsby* *The Hardy Boyds*		David Foster Wallace	
MATH & SCIENCE						
Principles & Theory	Physics Chemistry Marie Curie	Algorithms	Statistics/Probablity	Random numbers Chemistry: Pharmacutical engineering and food science	Random numbers Linear Algebra Binary Nuclear Engineering	Random numbers Chemistry in relation to mental illness Revision/debunking/disproving old theories of math and science
BUSINESS & PROFESSIONAL						
Startups		Startup failures	How to create a startup	Ideas	Difficulties/failures/recession	Silicon Valley
PERSONAL CARE						
Food/nutrition					Eating healthy	Drugs
Mental health	"What is Life"	Psychology Thought Control	Meaningfulness of life, Loneliness	Popularity		
Intelligence			Geniuses	Nerds	Non-human intelligence (animals)	
POPULAR PEOPLE	Einstein	Steve Jobs, Bill Gates	Steve Jobs Bill Gates	Paul Graham Alan K Bill Gates Einstein	Bill Gates	

References

About Y Combinator. (n.d). *Y Combinator*. Retrieved from https://www.ycombinator.com/about/

Amazing, Magnificent Reverse Job Application. (n.d.). Retrieved from https://web.archive.org/web/20181227023957/http://reversejobapplication.com/

Andrew Horner and the Fantastic, Amazing, Magnificent Reverse Job Application. (n.d.). Retrieved from http://www.reversejobapplication.com/ Andrew Horner and the Fantastic,

Bachmann, M. (2010). The Risk Propensity and Rationality of Computer Hackers. *International Journal of Cyber Criminology*, *4*(1&2), 643–656. Retrieved from https://pdfs.semanticscholar.org/bf09/3c90e7cba8c50b1244db02902973f3f5d896.pdf

Bio. (n.d.). *Paul Graham*. Retrieved from http://www.paulgraham.com/bio.html

Bortnik, S. (2013, November 6). Five Interesting Facts about the Morris Worm (for its 25th anniversary). *WeLiveSecurity*. Retrieved from https://www.welivesecurity.com/2013/11/06/five-interesting-facts-about-the-morris-worm-for-its-25th-anniversary/

Blackie and Son. (2013). Blackies' Dictionary of Computer Science. Retrieved from https://books.google.com/books?id=P2EtDAAAQBAJ&pg=PA103&dq#v=onepage&q&f=false

Chen, Q. (2018, February 22). #CodingIcon: Suz Hinton - Nice Cyber Human. *jewelbots*. Retrieved from https://jewelbots.com/blogs/jewelbots-jems/codingicon-suz-hinton

Chiesa, R. (2010, July). Interview with a Hacker: Chronicles of a Black Hat. *Freedom from Fear*, *7*, 5. Retrieved from http://f3magazine.unicri.it/?p=333

Coleman, T. (2013, April 11). Kevin Mitnick the Hacking Hamburglar. *Forbes*. Retrieved from https://www.forbes.com/sites/singularity/2013/04/11/kevin-mitnick-the-hacking-hamburglar/#dbb733f4ac99

CyberSecurity. (n.d.). A Brief History of Hacker Culture. *Cyber Security Masters Degree.org*. Retrieved from https://www.cybersecuritymastersdegree.org/a-brief-history-of-hacker-culture/

Encyclopedia Britannica. (2019, March 8). Bill Gates: American Computer Programmer, Businessman, and Philanthropist. *Encyclopedia Britannica*. Retrieved from https://www.britannica.com/biography/Bill-Gates

Graham, P. What I've Learned from Hacker News. (n.d.). Retrieved from http://www.paulgraham.com/hackernews.html

Graham, P. (n.d.). Hacker News FAQ. *Y Combinator*. Retrieved from https://news.ycombinator.com/newsfaq.html

Graham, P. (n.d.). Hacker News Guidelines. *Y Combinator*. Retrieved from https://news.ycombinator.com/newsguidelines.html

Graham, P. (n.d.). Why YC. Retrieved from http://www.paulgraham.com/whyyc.html

Graham, P. (2004). Great Hackers. *PaulGraham.com.* Retrieved from http://paulgraham.com/gh.html

Graham, P. (2007). Startup News Becomes Hacker News. *Y Combinator*. Retrieved from https://news.ycombinator.com/hackernews.html

Greenberg, A. (2014, September 24). Kevin Mitnick, Once the World's Most Wanted Hacker, is Now Selling Zero-Day Exploits. *Wired.* Retrieved from https://www.wired.com/2014/09/kevin-mitnick-selling-zero-day-exploits/

Harvey, B. (1985). What is a Hacker. Retrieved from https://people.eecs.berkeley.edu/~bh/hacker.html

Himanen, P. (2001). The Hacker Work Ethic. In *The Hacker Ethic and the Spirit of the Information Age.* New York, NY: Random House. Retrieved from https://archive.nytimes.com/www.nytimes.com/books/first/h/himanen-hacker.html

Isaacson, W. (2015). The innovators: How a group of inventors, hackers, geniuses and geeks created the digital revolution. London: Simon & Schuster.

James Somers. Retrieved from http://jsomers.net/

James Somers. *LinkedIn.* Retrieved from https://www.linkedin.com/in/james-somers-4703364/

Kelty, C. M. (n.d.). *Limn.* Retrieved from https://limn.it/articles/the-morris-worm/

Lee, T. B. (2013). How a Grad Student Trying to Build the First Botnet Brought the Internet to its Knees. *The Washington Post.* Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/

Legendary Hackers. (2010, August 23). Retrieved from http://www.autistici.org/rez/hackers.php

LulzSec. (2019, February 15). Retrieved from https://en.wikipedia.org/wiki/LulzSec#Ideology

Manalac, K. (2016, August 11). YC Offices in 11 Countries this Fall. *Y Combinator*. Retrieved from https://blog.ycombinator.com/yc-office-hours-in-11-countries-this-fall/

Matulessy, A., Humaira, N. H. (2016). Hacker Personality Profiles Reviewed in Terms of the Big Five Personality Traits. *Psychology and Behavioral Sciences*, *5*(6), 137-142. Retrieved from http://article.sciencepublishinggroup.com/html/10.11648.j.pbs.20160506.12.html

People. (n.d.). *Y Combinator*. Retrieved from https://www.ycombinator.com/people/

Peter, K. (1980). The Hacker Papers. *Psychology Today*. Retrieved from http://www.textfiles.com/news/hackpape.hac

Peterson, A. (2015, November 5). Inside the Economics of Hacking. The Washington Post. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2015/11/05/inside-the-economics-of-hacking/?utm_term=.ab43161782da

Power, K. (2016, August 17). *Tripwire*. Retrived from https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-evolution-of-hacking/

Rao, L. (2013). The Evolution of Hacker News. *Tech Crunch*. Retrieved from https://techcrunch.com/2013/05/18/the-evolution-of-hacker-news/

Raymond, E. (n.d.). Gender and Ethnicity: Appendix B. A Portrait of J. Random Hacker. *The Jargon File (version 4.4.7)*. Retrieved from http://catb.org/jargon/html/demographics.html

Raymond, E. (n.d.). Personality Characteristics: Appendix B. A Portrait of J. Random Hacker. *The Jargon File (version 4.4.7)*. Retrieved from http://catb.org/jargon/html/personality.html

Raymond, E. (n.d.). Politics: Appendix B. A Portrait of J. Random Hacker. *The Jargon File (version 4.4.7)*. Retrieved from http://catb.org/jargon/html/politics.html

Raymond, E. (1996). The New Hacker's Dictionary. *The MIT Press*. Retrieved from https://books.google.com/books?id=g80P_4v4QbIC&pg=

Raymond, E. S. (2001). How to Become a Hacker. Retrieved from http://www.catb.org/~esr/faqs/hacker-howto.html

Raza, A. (2016, January 21). 10 Most Notorious Hacking Groups. *Hack Read*. Retrieved from https://www.hackread.com/10-most-notorious-hacking-groups/

Sloat, S. (n.d.). 'Social Banditry' Theory Explains Why So Many People Are Supporting Anonymous. Retrieved from https://www.inverse.com/article/36123-anonymous-supporters-social-banditry-theory

Symantec. (n.d.). What is the Difference Between Black, White and Grey Hat Hackers?. Retrieved from https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html

Systers. (n.d.). Retrieved from https://anitab.org/systers/

The Hacker Classics. (n.d.). Retrieved from http://jsomers.net/hn/

The Mentor. (1986). The Conscience of a Hacker. *Phrack Inc, 1*(7). Retrieved from http://phrack.org/issues/7/3.html

Ward, M. (2011, June 9). A brief history of hacking. *BBC News*. Retrieved from https://www.bbc.com/news/technology-13686141

What Happens at Y Combinator. (n.d.). *Y Combinator*. Retrieved from https://www.ycombinator.com/atyc/