The New Computer Hacker's Quest and Contest with the Experienced Hackers: A Qualitative Study applying Pierre Bourdieu's Field Theory

Michael Nycyk[1]
Curtin University, Australia

Abstract

Hacker forums are places for new hackers, newbies, to find information on hacking practices and to become part of a community. This study contributes to understanding ways newbies try to become accepted experienced computer hackers. Using Pierre Bourdieu's Field Theory and its concepts, 500 threads from a forum were analyzed to see how newbies attempt to gain a place in the hacking field amongst experienced hackers. Thematic analysis methods were used to demonstrate how the forum's field, and those within it, behaved to obtain what Bourdieu describes as cultural and social capital to obtain knowledge and skills to hack and become accepted hackers. The significant finding was the theme of contesting social capital. This showed the types of strategies employed by experienced hackers to prevent or hinder newbies obtaining the skills and knowledge, social capital, to achieve their hacking goals. This study gives insights in to new hacker's motivations and strategies for becoming accepted hackers and gives suggestions for further research in this growing area.

Keywords: Bourdieu, Contestation, Field, Habitus, Hacker Forums, New Hackers (Newbies), Social and Cultural Capital.

Introduction

The considerable body of literature seeking to understand computer hackers' motivations and behaviors still needs further inquiry as hacking cyber crime grows in sophistication and geographic reach (Décary-Hétu & Dupont, 2013; Nikitina, 2012; Turgeman-Goldschmidt, 2008; Yar, 2005; Taylor, 1999; Jordan & Taylor, 1998). Needing further investigation is the area of new computer hackers or newbies. This study specifically examines newbie hackers' acquisitions of skills and knowledge in their interactions with experienced hackers in a public hacker forum. The framework this study uses is Field Theory by Pierre Bourdieu (Bourdieu, 1990; Bourdieu, 1985; Bourdieu, 1977) with an emphasis on hackers' skills and knowledge trading, the cultural and social

[1] Consultant Researcher, Department of Internet Studies, School of Media, Culture and Creative Arts, Curtin University, Perth, Western Australia. E-mail: michael.nycyk@gmail.com

capital of the field (Bourdieu, 1986; Bourdieu, 1984), between newbies and experienced hackers.

Although social media sites such as Facebook and Twitter are used by hackers, online community forums are still utilized as spaces hackers gather online (Kubitschko, 2015). Newbies join to gain access to highly specialized skills, information-sharing, networking and support from experienced hackers (Turgeman-Goldschmidt, 2008; Meyer & Thomas, 1990) but may experience admonishment, mocking and insults for their lack of skills and types of questions they ask (Décary-Hétu & Dupont, 2013; Meyer & Thomas, 1990). Hence the field of the forum operates on power relations; that is, in Bourdieu's terms (1990), the capital of skills and knowledge is contested by newbies because they want what the experienced hacker possesses. This exploratory study focuses specifically on this aspect. Research on newbies has not adequately focused on describing and analyzing the relationships between newbies and experienced hackers in online community hacker forums.

The investigation of hacker forums to discover their characteristics and activities for cyber security has previously occurred. For example, Imperva, a global computer network security company, conducted a qualitative content analysis of threads within a large hacker forum. Their report identified descriptive trends, such as increased Structured Query Language (SQL) injections discussions to cause Denial of Service (DoS) attacks to a noted increase in newbies joining the forums from previous years' analyses (Imperva, 2012). Although using a considerably larger sample size than this study, 250,000 members' threads were examined (Imperva, 2012), it is clear that hacker forums require further analysis to give computer network security professionals insights into hacker behaviors and identify trends in hacker culture.

Newbie hackers desire to be a part of a hacking community even if their individual goals differ. Hackers' desire, as Nissenbaum (2004) describes, total and free access to computers and information, and mistrust centralized authority, have a disdain for obstacles erected against free access to computing and desire to be evaluated by their technical virtuosity and accomplishment. Hackers hack for reasons such as: conflicts with authorities and revenge motives (Chiesa, Ducci & Ciappi, 2009), beliefs that breaking into computer systems benefit society by showing how to increase computer security (Kao, Huang & Wang, 2009), achieving feelings of power due to low self-esteem (Fötinger & Ziegler, 2004), gaining entrance to a social group (Kilger, Stutzman & Arkin, 2004) and to satisfy an addition (Taylor, 1999). These also play a part in a desire newbies have to join a hacker community and work with experienced hackers to learn skills and knowledge to hack computer systems.

Yet newbie hackers face a constant battle to be accepted by hackers from the beginning of their quests to obtain the capital they need to hack. For example, experienced hackers resent script kiddies and unskilled hackers who use hacking tools such as code and scripts developed by experienced hackers. In a display of power by experienced hackers, script kiddies are identified, shamed and called pestilence and other terms, and banned from hacker communities (Taylor, Fritsch, Liederback & Holt, 2011). Hacker ethics, rules hackers in the particular community abide by, vary, and experienced hackers will often want proof from the new hacker, such as completing a fake or real hacking mission, before joining. Newbies may resent such activities to enter the field, but will contest the knowledge and skills of the experienced hacker by posting threats, abuse, and pleas or try to outsmart hackers with superior displays of knowledge.

The research problem explores the relationships between the newbie hacker and experienced hackers in one public hacker community forum. There is, in Bourdieu's (1986) terms, a contestation over capital because newbies struggle to gain acceptance and obtain the hacking knowledge and skills to be a part of a hacker community. They also experience ridicule, shame and abuse if they violate not only the formal rules of a hacker forum but also the beliefs and ethics of the group. This study uses hacker forum threads as data like Décary-Hétu & Dupont's (2013) study. Other studies, such as Bachmann's (2010) survey of hackers at a conference, and Shachaf and Hara's (2010) and Turgeman-Goldschmidt's (2008) interviews of hackers' motivations and behaviors were effective in gaining insights into hackers' worlds. Using textual data only can be just as valuable despite some concerns that will be addressed in the methods section.

This study is guided by three research questions which aim to describe and analyze newbies and experienced hackers interactions as the newbie tries to obtain knowledge and skills, the capital of the hacker forum. These questions are:

1. What are the types of capital, skills and knowledge, newbies seek and how do they seek them?
2. How do newbies challenge the established order of the hacker community forum and what strategies do experienced hackers employ to maintain power and control over newbies?
3. What insights can be drawn from these forum interactions on the relationships between new and experienced hackers?

The study's framework is based on Bourdieu's Field Theory, the elements of which are discussed here.

Framework: Bourdieu's Four Elements of Field Theory

Four of Bourdieu's concepts create a framework to investigate this research problem. These are: field and habitus, which allow a rich description to be made of what the group is doing in the field, and social and cultural capital which are types of resource gained on attaining group membership (social) and forms of knowledge and skill that allows a person a greater financial or social status in a group (cultural) (Bourdieu, 1990, 1986, 1984; Bourdieu, 1977). Central to this research is how power operates; that is, the power experienced hackers have to control what newbies need to do to obtain capital, but also how newbies will challenge the established order to attempt to obtain capital.

Field

Bourdieu explains a field as a system where social positions exist structured internally by hierarchical power relationships (Bourdieu, 1990, 1984) much like a football game field. It is a space where struggles over the appropriation and acquisition of capital occur. In the context of the hacker forum, the posts on the forum threads are the space where the hackers communicate, but these also exert power relationships over newbies by the words posted in the thread. First, newbies want knowledge and skills to hack, obtaining social capital, but struggle because they may not receive the answer they want. Second, they also want to be accepted and be taken seriously, which also a struggle because they may be dismissed by experienced hackers and not allowed to advance in the hacker field.

The comparison between newbies and hackers is described as a power relation because one group has control over the actions of another, much like Bourdieu says exists in the legal system where judges have control over the actions of lawyers (Bourdieu, 1984). Newbies can advance in the hacker community field, which is symbolized by the removal of the word newbie off their post and replaced with hacker, by the completion of hacker missions and contributing more than two posts to a thread. This advances their position in the field as it means they can access more features in the forum such as the ability to become administrators and remove or warn newbies if the newbie acts inappropriately.

Habitus

While field describes the space activities are occurring, habitus describes the individual's values and expectations aligned with the social group they are a part of (Bourdieu, 1990, 1984). Bourdieu's critics clarify habitus as the habits and dispositions, ways of acting in certain ways that always occur (Hanks, 2005). Describing habitus accounts for the reproduction of social and cultural domination because people must act in a certain way to be a part of a group and demonstrate this to others (Mander, 1987). Habitus is a product of the environment people operate in often determined by pre-existing values those in the field have. It is contested when people want change or when a group changes their habits or values as society or their circumstances around them changes.

Habitus describes particularly well how the values, habits and dispositions of one group, the hackers, impact on another, newbies. Habitus insists people in a group think and act in certain ways or they cannot gain the capital they desire (Bourdieu, 1986, 1984). Giving capital to others is influenced by the group's habitus. For example, experienced hackers want newbies to act in ways that do not waste their time, which is an established habit to deride newbies if they do, and newbies have difficulties working out what these are. If the newbie does not align themselves with the group's habitus the result is they will not obtain the capital they need to hack.

Social and Cultural Capital

Capital is the skills and knowledge embedded in the group members' field possessed by everyone but at different levels, which determines their position in a field. Using Bourdieu's (1986) formal definitions for this study, the two types of capital defined are:

1. Cultural Capital: The forms of knowledge, skills, education, and advantages that an individual has, which give them a higher status in a society or field

2. Social Capital: The resources available to an individual on the basis of honor, prestige or recognition, and serves as value that one holds within a culture

In this study the cultural and social capital are the skills and knowledge of hacking systems, combined with information about the formal learning needed to hack and the attitudes and values of the larger hacking community. To obtain capital, as Bourdieu (1986) argues, depends on skill and performance in the field. However, newbies may not be satisfied with these demands and contest the field.

It is this contestation over capital which is important to describe and analyze. The struggles newbies have will depend on their willingness to conform, but if they do not receive the capital they need they can argue with other hackers in the threads. Sometimes

a contestation over capital means the field will change when those in it see the unfairness of their decisions. Nevertheless, withholding capital can also have some positive effects, such as newbies can give up their aspirations to hack and potential cyber crimes can be avoided as they are discouraged by hackers.

Method

The section describes and discusses the methods used to investigate the hacker forum and Bourdieu's concepts, using the rigorous and most appropriate method, Thematic Analysis (Braun & Clarke, 2006). This method aims to understand current practices of individuals, allowing the detection and identification of factors that influence issues generated by those in the field or group (Alhojailan, 2012). It identifies, analyses and reports patterns or themes within a data set in detail but also helps interpret various dimensions of the research problem (Braun & Clarke, 2006).

First, a public hacker forum was identified which was representative of a field where newbies seek capital. For anonymity, the site is not named in this paper to protect informants. However, the posts can be viewed by the public but as an added consideration in the data examples the user names are left out. The data are reliable because members have to join the forum to post. A total of 500 posts were chosen at random from the forum with the main criteria that a newbie posted in the threads. Once collected the data were analyzed with qualitative software.

Second, the method chosen, thematic analysis, is appropriate because it involves searching across a set of data to find repeated patterns of meaning (Braun & Clarke, 2006). Two advantages are: it suits finding evidence of the operation of Bourdieu's framework, field, habitus, social and cultural capital, but also opens the possibility of finding other unexpected themes that answer the research questions.

Undertaking thematic analysis involves a number of steps. Thinking about concepts being sought, guided by the questions and framework, categories of each concept are created using a deductive approach in finding them. The data are then coded to the concept, with the creation of categories and subcategories that clarify and explain the concept. Importantly, and what contributes to the rigor of the study, is pattern finding and constantly going over categories to compare and contrast data to demonstrate with evidence what is occurring (Braun & Clarke, 2006). The iterative process is time-consuming, but by not rushing it allows assumptions about category and data examples to be clearly explained and justified. The categories and then summarized and titled with a named category and a number of elements identified that describe the theme.

Ethical considerations of using data from a public online community site for this study need clarification. Kollock (1999) warned that digital artifacts researchers use can subject the informants to surveillance. With more sophisticated tracking and data mining software available, Skågeby (2015) cautions that forum search engines are now sophisticated to the point they can pick up exact text of informants.

The study is still considered low-risk, but precautions were used to preserve as much anonymity as possible. Using advice from Markham and Buchanan (2012) of the Association of Internet Researchers, Madge (2007) and Bruckman, (2002), these strategies where used to minimize informant risk:

1. The site is officially and publicly achieved.

2. No password is required for accessing it nor joining the site as a member should occur.
3. No site policy prohibits using data for research purposes.
4. The topic is not highly sensitive.

In the results section although the text is reproduced leaving out usernames assisted with protection of posters. It is also argued that the data are public but the risk of those seeking those who posted for criminal prosecution is likely non-existent.

Results

The findings suggest that Bourdieu's contestation over capital is explicitly shown in the interactions between experienced and newbie hackers in the field of the hacker community forum. An overall description of the major theme is that experienced hackers will use their cultural and social capital they possess to either advance or suppress the advancement of the newbie. As Bourdieu (1990, 1986, 1985) argues, having a form of power over what others want means those entering the field have to negotiate it by adhering to established rules. This power held by the experienced hackers was identified as the requirements newbies must achieve before improving their position in the hacker forum field.

This observation was evidenced in four themes, one from cultural capital, the experienced hacker's forms of knowledge and skills giving them a higher status in the community (Bourdieu, 1990, 1985), and three themes from the social capital concept which are the resources that newbies can obtain based on group membership participation and co-operation. The types of capital, skills and knowledge newbies seek and how they are sought is answered by both the interchange of hacker advice, technical advice and experiential advice, through interactions within threads.

The second research question was answered by the fourth theme showing the level of contestation over capital. Newbies challenged the established order of the hacker community by asking questions which caused the experienced hackers to use their positions to stop these behaviors. For example, even with the explicit rules in place for using the community, newbies do make requests for hacking techniques and procedures which should advance their position to go and hack but are disallowed. What was unexpected was the level of protectionism of the forum with consistent admonishment if illegal activities were mentioned by newbies. Hacking, despite years of claims from hackers to the contrary, is still seen as a 'criminal act' to be feared, a form of social deviance and a threat to world information systems security (Dremliuga, 2014; Kirwan & Power, 2013; Taylor et al., 2011; Kshetri, 2010; Warren & Leitch, 2009; Flowers, 2008; Mitnick, 2002).

The results showed that the experienced hackers will advise newbies how to hack, including posting programming code and Structured Query Language (SQL) database hacking codes, yet in turn will use the power they have gained to censor and admonish newbies who ask for such knowledge. This group protects their interests in the field and will prevent illegal activities being discussed. Yet newbies do get confused about how to act is evident despite the rules of behavior and participation clearly posted on the forum's site. The site displays the warning "The Site Does Not Support Legal Activities" but is clearly ignored in the sample of threads. In the field the identified struggle, as Bourdieu

uses that word, is the contradiction that newbies must learn the habitus of the community yet often choose not to do so hence limiting their acquisition of capital.

The four themes identified from the analysis and their components are presented in Table 1. Cultural Capital only occupies one significant them, while themes two to four are findings about Social Capital:

Table 1. Capital Type, Theme Names and Theme Elements

Capital Type	Theme Name	Theme Elements
Cultural	Impart Skills and Knowledge	• Give advice and knowledge to maintain skills • Possess specific skills sought after • Use skills to advance position in field
Social	Advice Seeking	• Newbie freely given needed information • Newbie seeking specific information • Newbie wants learning advice • Newbie wants starting point for hacking
Social	Advice Giving	• Give needed information freely • Impart experience • Solve a problem for another
Social	Contesting Social Capital	• Admonish, insult and humiliate newbies • Experienced hackers criticisms of newbies' behaviors • Newbies' criticisms of community rules • Warning newbies of illegalities and punish them

These results are now discussed in-depth. The third research question about the insights drawn from the study is discussed in the results section.

Theme 1: Impart Skills and Knowledge

The theme describes the types of cultural capital held by the experienced hackers that demonstrates how they maintain the position in the field they occupy. Their acquisition of hacking skills and knowledge is sort after by newbies and is exercised in the willingness of the hacker to impart this capital by posting it in the threads. In giving advice it is bestowing information and knowledge, therefore capital, onto others to advance their position while maintaining their own skills in the field. The hacker and newbie are identified by numbers as different ones were analyzed in each exchange. This example demonstrates an advice interchange:

HACKER 1: As mentioned above python is a great language to start learning. If you choose to learn it I would recommend lawofcode.com and for books 1.Learn Python the Hard Way by Zed Shaw 2. Violent Python (and/or) Gray Hat Python. In that order btw.

Maybe something in the following order
1. Codecademy
2. Learn Python the Hard Way
3. Read - Violent Python (Hacking with Python ebook)

NEWBIE 1: You really helped me out :) Thank you!

By recommending resources to the newbie, the hacker shows those in the community they know the exact resources that can advance another hacker. This is interpreted in Bourdieu's (1985) theoretical terms as the distribution of capital as an instrument for the appropriation of the product of labor which is defining the state of the power relations occurring in the field and the position of the person in the field. This simple information interchange does potentially change the position of the newbie who may take the advice and use it. This type of attempt at advancement in the field was seen throughout the data and demonstrates how it was consistently operating.

When cross-checking the data that makes up the themes, a subtle overlap was seen between cultural and social capital when an element of this theme was identified. The majority of newbies wanted specific skills and advice. Hackers would provide complex and detailed posts on how to hack. In this example an experienced hacker gives information on the correct code to hack a file:

HACKER 2: A local file inclusion means that it is possible to load some local file (a file on the machine) in some given path or input, allowing the hacker to read the contents of the file.
An example of expected input using a $_GET parameter

Code: Select all
https://www.yoursite.com/members.php?member=pythonhacker

Malicious code:
Code: Select all
https://www.yoursite.com/members.php?member=../../../../../../etc/passwd%00

The experienced hackers also used such information to advance in the field by completing more complex hacking missions set by the community and interacting with experienced hackers to give their experiences of the hacking mission. A posting which shows this is a hacker developing code for others to use:

HACKER 3: Here's an example I made real fast in case you are interested.

Code: Select all
import httplib2
#import re

```
h = httplib2.Http('.tmp')
response, content = h.request('http://checkip.dyndns.org')
print((str(content).split(": ")[-1]).split("<")[0])
```

Any C++ compiler should be able to compile C code just fine

The conclusion of this theme is that the cultural capital that the hackers post in the community can earn them a higher and more credible status amongst others. They are genuine postings to help others hack, but do function as capital growing that earns respect from other hackers in the community.

Theme 2: Advice Seeking

The giving and receiving of advice on how to hack, and on hacker philosophies and rules, underpins the growth or loss of social capital in this community. The habitus of experienced hackers is to help others, but only under certain defined assumptions brought to the community. Hackers, regardless of their status of being called white (good), black (bad) or grey (elements of both) do foster an informal but powerful collective worldwide community by frequent swapping of capital online and through hacker conferences or publications of experiences in books and other written means (Holt, Strumsky, Smirnova & Kilger, 2012, Chiesa et al, 2009; Schell & Dodge, 2002; Jordan & Taylor, 1998). The type of social capital sort are hacking skills and knowledge, but in order to obtain it the advice must be worded correctly within the boundaries of the hacker community or it is withheld.

Four elements of advice seeking were identified. First, the newbie is given the information freely without the expectation of even a thank you to the hackers, although many did thank those who gave the advice. Here a hacker freely gives information on how to fix an operating system issue:

> HACKER 4: This isn't something that should happen on a normally functioning system. In your first post, you said you had recently installed windows7. If it was me, considering how frequently i use the browser and how suspicious this is, and since i have the installation cd, I'd do a fresh install again. That's all I've got. Good luck bro.

Further examining this theme, the continuous advice seeking was seeking specific information, for example how to remain anonymous online, SQL code for hacking databases or what hacking tools could be obtained to hack systems. Newbies consistently sought specifically how to remain untracked by authorities and others by using a proxy server, which can connect their computer to other indirect network connections to other networks services to hack. This example of specific information seeking generated much advice and was a frequent request newbies made in the community seeking hacking knowledge:

> NEWBIE 2: I thought this might be the best place to ask this. What's the best way to hide yourself online so that people who might be looking for you can't track you when you're doing "stuff"? ok I guess I don't care if they know I'm online... I just don't want them to be able to track me.

Some questions suggested the newbie knew certain information already, as shown in this example where a more specific question about anonymity was asked:

> NEWBIE 3: If i spoof my MAC address and use an unencrypted and public network access point, is there any way to connect me to my actions?

Nevertheless, all advice seeking posted was responded to and no newbie was criticized for asking about topics, although the way they asked questions caused friction as will be seen in theme four.

Aside from skills, newbies sought general advice about learning to hack, as in what programming languages and hacking techniques were needed, and what was a starting point to hack. This was seen as important social capital for those how joined the community to begin hacking. In this representative example, the newbie asks what is valuable to learn to continue hacking:

> NEWBIE 4: I don't know if I'm in the right path on becoming a hacker. I'm a 3rd year college student and the language I only know is Java. I know a little about HTML, CSS and JavaScript because we have a web development class in our college. Will I continue learning Java? Because almost all the posts I've seen here suggests learning C or C++.

By contrast, many newbies may have known of hacking tools and programming languages, but still needed a starting point. In this example, which experienced hackers would often respond kindly to, the newbies would ask similar type questions on how to start hacking:

> NEWBIE 5: Hi guys, I'm new here and recently I've been wanting to learn network security and pen testing. In the past I've worked a bit with some basics of SQL Injections and some metasploit but that's about as far as my experience goes. As for programming, my knowledge is close to non-existent. So my question is, where do I go from here?

Overall, this theme captures the type of capital that is sought by newbies to advance their positions as hackers in the community and outside of it. The next theme that arose demonstrates how the hackers advance a newbie's acquisition of capital by giving advice.

Theme 3: Advice Giving

This theme demonstrated that experienced hackers in the community would give detailed advice freely on how to solve problems and warn of the pitfalls and challenges a newbie can experience hacking. They also imparted their experiences of hacking, not just practical skills to hack, but also the experiences and philosophies they had hacking. The information to hack was given freely, yet the hacker would warn the newbie if the activity was illegal. In terms of social capital, advice given is valuable to newbies and is crucial to their advancement in the field. Two examples of freely given information were:

1. HACKER 5: This is a very neat tool a friend introduced me to. Depending on what 'nix OS you're rocking, it may have a different name. You may just have to Google it to find which one goes with your OS. But anyway, this

tool sets a terminal to drop down at the press of a button, then wrap itself up and get out of your way when you press it again.

2. HACKER 6: What specifications are you looking for? Just for a run of the mill website with nothing fancy, check out http://www.freewebs.com

Hackers would also give advice to newbies based on their experiences of being a hacker and the field they occupy. The data also suggest this is the way hackers impart their habitus to the newbie expecting it to be respected, reinforcing the boundaries of the field (Bourdieu, 1986, 1985, 1977). These examples illustrate this:

1. HACKER 7: Hacking is like a tool it can be used all kinds of ways. In some cases yes it can destroy privacy, for instance the NSA using a JavaScript exploit to find people on tor. As far as learning to do this though what better way to protect your own privacy than to learn how to break it. Similarly the purpose of a learning a martial art is probably not to go around beating the crap outta peoples. It can be about exercise, self-defense, competition etc. In general this site also teaches the hacker mindset, thinking out site the box and finding clever solutions to problems, and provides a community of people with similar interests.

   2: HACKER 8: Python is a great language to start with, it's not terribly difficult, resulting code is pretty easy to read, and it's powerful to boot! Where are you in the Codecademy course, and what exactly are you having issues with? My python is a tad rusty, but I don't mind giving you advice!

The first example imparts general knowledge about hacking activities whilst the second imparts experience with a programming language which the hacker is willing to share with the newbie. Both are social capital because they are imparting advice and knowledge the newbie can use practically to advance their position in the field.

A main element of this theme was the gaining of social capital through the solving of hacking problems. The first example shows a hacker advising a newbie about how online website forms can be hacked because the newbie had their website hacked through this method and wanted to know why it happened. The second example came from a newbie who was hacked and wanted to minimize the attacks that their system was experiencing:

1. HACKER 9: It may be that the search field, or any field in the forms that allow user input have not been properly sanitized to protect against JavaScript injection, i am speculating because the website is not in my native language and i can't check it out. If this is the case then a visitor could even post a comment with html meta tags and redirect every one or any number of things with JavaScript...

2. HACKER 10: You can use a virtual machine and load the same protected image each time you use it, effectively starting with a clean slate. This offers some modicum of protection from tracking cookies, malware, etc.

The information needed is given freely with the choice for the newbie to act on it. This did not always mean the newbie returned to the forum to continue interacting, but

the presence of hackers who gave advice freely, imparted their skill and philosophical advice and solved newbie problems, was highly valued. However, as seen in theme 4, this capital was contested. Whereas themes 1 to 2 suggested a highly co-operative field where capital was easy to obtain, which answered the first research question of what types of capital could be obtained and how newbies obtained it, newbies did challenge the field for resources which lead to hackers protecting it.

Theme 4: Contesting Social Capital

This theme demonstrates the operation of power over newbies when social capital is contested. In this sense, contestation means challenging the established order of a field to obtain capital. The practice the first three themes showed was the operation of habitus; the history of the community was to produce and reproduce collective practices which insist on what Bourdieu (1990) states is a correctness of practice. Up to this theme the newbies mostly co-operated by doing the practices the field demanded to advance from the newbie to hacker title. Clearly, some newbies either did not know how to ask in specific ways questions about hacking or were impatient, posting questions without reading the forum rules. When the hackers would not give them the advice or information they wanted, newbies would challenge the hackers, in turn the hackers used the collective habitus of producing strategic responses such as admonishment and other tactics to maintain power and control over the newbies.

Contestation is a struggle in the field for capital (Bourdieu, 1990) and operates in this hacker community by four elements. The first element is by using admonishment, insults and humiliation against newbies. One noticeable strategy employed as a warning to newbies was the yearly 'Idiot of the Year' prize voted by the hackers as the worst of the year:

> HACKER 11: It's about time to continue tradition with our Idiot of the Year contest. Voting ends on December 31st or January 1st, depending on your time zone. With the seemingly decreasing activity in the forums, there have been a less amount of good idiot. So from the idiots that we do have, pick wisely!

The next two were frequent examples of admonishing newbies, using insults and humiliation, as tactics to reinforce the community's habitus of newbies conforming to certain rules and losing capital if they did not comply:

1. HACKER 12: First of all.. Don't post in colors. It looks retarded.

2. HACKER 13: Ok you are new. You need guidance. Firstly we don't talk like that, and using colours and lots of emoticons. This is what you should have said:

> SAME HACKER 13: wrote:
> I don't know what the hell I'm doing. I'm really good with computers but I've never seen this type of thing before. Could someone please help me? Please!
>
> Ok that is much easier to understand, so please type like that in future.

Using abusive language and name-calling to admonish was frequent as this example shows:

> HACKER 14: My first impression was that you're an idiot, but it quickly came to light that you are in fact a moron.

The struggle for the newbies here was to make the choice to endure the abuse and apologize or not reply and go to other hacker forums. It still meant that they did not receive the capital they needed to advance their hacker knowledge.

As part of their habitus, hackers also would criticize newbies for the wording of the questions the newbies would post. If the post asked for advice deemed illegal the hackers would warn, admonish and sometimes ban newbies. This was strongly tied to the constant need to enforce the image of the hacker community as being 'legitimate' and not encouraging criminal behaviors. If the newbie criticized the rules they would be admonished. These four examples show the operation of power in the field as newbies are criticized for their posts:

1. NEWBIE 6: well tbh thought this was a hacker community, but you can't ask for specific downloads or help, even the admins refuse to give some good information, you call yourself hackers but I'm sure only 0.5% of these people is worthy to be called one, I'll be leaving this site to join a real community where people help each other instead of being scared to something wrong. hail black hackers and hail my old community where you had special room to insert sites / people that needed to be dealt with

2. HACKER 15: The fact that I haven't seen it, doesn't mean it doesn't happen (though I doubt that). Either way, no-one will help you do something illegal here. At best a mod will come along to lock this thread and move it to the graveyard, at worst you will be banned from the site too. We'll see what happens...

3. HACKER 16: I am a professional hacker. Let's not talk about "illegal activities" on a "hacking form" pm me

   I don't understand why this even has to be explained. It should be common sense.

   These are the type of people who deserve to be caught or scammed.

4. HACKER 17: On a hacker's forum, you really shouldn't really say that. Should the party van catch someone who's part of this community, we won't look like saints either, you know?

   Notice the disclaimer at the bottom of this page: (community name) does NOT condone or support illegal activities. Seeing as you have so much time on your hands, you should be able to figure it out yourself if it's really that pressing of an issue. While you sound benign, you could be attempting to bring down the network/wreak general havoc, etc. Sorry, but seeing as this is likely to be illegal, we can't really help you.

This contestation raises some questions as to why newbies choose to challenge the field. As it is working from text, the reasons may not be clear but in reading the posts the suggestion is that newbies just did not read the taken-for-granted community rules. It also calls into account newbies' motives. Some of the newbies' requests fall into the category of acts of force or fraud undertaken in pursuit of self-interest, or criminality, as defined by Gottfredson and Hirsch (1990). Even with explicit rules for behaviors, some may view even this public community as a source of black hat activity. However, although there is conflicting information; that is, the hackers do tell people specific hacker methods, this contestation of the hackers protecting the community show they create a community of practice that is creating ethical frameworks to guide field activities (Pike, 2013).

New and established hackers believe they may gain respect and recognition from hacker peers (Young, Zhang & Prybutok, 2007). Yet obtaining this capital is often a struggle for the newbie if they do not follow or know the established rules of the field. It can be a counter-argument that many do not take the time to study the rules of a field and eagerly rush in. This can be assumed in reading the posts. However, what is evident from the results of this theme is that contestation is a powerful struggle. The community welcomed newbies but did not hesitant to give out punishments, including banning newbies. Bourdieu (1977, p. 40) illustrates the operation of a contestation over capital in a field that supports these findings:

> To possess the capital of authority necessary to impose a definition of the situation, especially in the moments of crisis when the collective judgment falters, is to be able to mobilize the group by so lemnizing, officializing, and thus universalizing a private incident (e.g. by presenting an insult to a particular woman as an affront to the hurma of the whole group). It is also to be able to demobilize it, by disowning the person directly concerned, who, failing to identify his particular interest with the "general interest", is reduced to the status of a mere individual, condemned to appear unreasonable in seeking to impose his private reason - idiotes in Greek and amahbul in Kabyle.

Therefore, applying this to the forth theme, the moment of crisis is when the newbie requests illegal information or challenges the community; therefore, disowning the newbie is the response. Not obtaining social capital may not concern the newbie, but it is seen that the newbie is unreasonable and imposing their reason onto the community. As example 1 in this part of the analysis showed, newbies, and sometimes established hackers although only one instance was noticed, hit back at the community. It is important to get capital and to some newbies it is a devastating experience not to gain it and advance their own hacking cause in, or out of, the community.

Discussion, Conclusion and Directions for Future Research

This section discusses findings and conclusions, as well as giving direction on future research of newbie hackers, and answers the third question, what insights can be drawn from these forum interactions on the relationships between new and experienced hackers?

The sophistication and frequency of cyber attacks must start from the mind of the newbie as they seek skills and knowledge, the capital of the hacker field to hack (Décary-Hétu & Dupont, 2013; Yar, 2005; Taylor, 1999; Meyer & Thomas, 1990). Using the sample set of threads, this study gave insights into newbie hacker behaviors in an online

public hacker community. Using Bourdieu's Field Theory concepts, an overall thematic picture of what occurs in one public online hacker community emerged. The field is the hacker forum itself where it is compulsory to contribute to advance. Hackers reproduce habitus which newbies must adhere to in order to gain capital. Habitus was seen as dispositions to reproduce practices which kept the community being seen as a white hacker, ethical place despite giving specific advice on how to hack. Newbies had to navigate this process and act accordingly.

The thematic analysis discovered themes of the gaining and contestation of capital hackers and newbies wanted. Bruan and Clarke (2006) argue, this method allowed a rich description of the data set, which this method achieved in the four themes. However, there was more evidence of the operation of social capital rather than cultural capital. The process operating was that hackers had power to give capital as their cultural capital; their knowledge to give was high. In the other themes it was the social process of asking, correctly, for social capital in an 'ask and give' advice process. If this failed, which it frequently did, Bourdieu's contestation in the field concept was activated and often the newbie could not advance in the community or gain capital to hack. These results answered the research question.

What was not expected was the depth of conflict between the rules and ethos of the community site, seen in the habitus where hackers would admonish newbies and sometimes each other for perceived illegalities. Contempt for newbies who wanted things done for them without making effort occurred frequently. The skills and information given on the forum contained code, methods and techniques to hack a network, software or a device. Newbies did ask how to perform illegal hacking activities, consequently getting admonished and warned, yet the experienced hackers would tell each other specifically how to hack something. As Taylor et al. (2011) stated, experienced hackers will ban newbies and script kiddies who waste their time yet hackers still claim there is a form of community amongst hackers. A newbie may find such a community confusing and in the data they often begged for information but the hacker's choice to answer depended on the specific way the newbie requested something. This can be difficult and perhaps deters newbies to learn hacking.

The insights drawn from the forum interactions, the third research question, were that newbies must learn, as Bourdieu (1977) states, the 'rules of the game' in the field to advance their hacking activities and not challenge the others in the field. For example, although not frequent, some newbies expressed frustration that they were not being answered. Their complaints were often met with contempt though some hackers would be sympathetic and correct newbies' behaviors. It is difficult to ascertain confidently if this hacker community was encouraging criminal activity because of the continued stating some activities were illegal. However, newbies if they worked out the rules of the community and learned to ask questions correctly could advance quickly which was evidenced by newbies being given a new title such as Experienced Hacker on the forum. This was the best symbol of the acquisition of capital.

A limitation of the study is the questioning of results as being speculative because the data are only textual. This is a legitimate concern because unlike interviews researchers cannot always check details with participants. Not knowing the full outcome of some interactions could have led to speculation of what was going on, influencing rigor. However, it is argued that the posts gave accurate representations of the interchange, or

not, of capital acquisition, sharing and contestation over both capitals. Researchers undertaking most textual discourse analysis work can subject themselves to the criticism that they put their own meanings on the text not capturing what is occurring from the participant's point-of-view. Although valid, this study was aided in rigor by using a sociological framework and a strong qualitative research method, combined with good data reliability, to produce a thematic insight into the ways newbies operate when trying to gain entrance to a competitive field such as hacking. It is also fact that the greater the sample size, which would require more work to analyze, the more insights and frequency of occurring issues could be uncovered.

Future research would depend on the information security industry's resolve to stop hackers. From a research view, perhaps a larger sample would give even more insights and show patterns a smaller study like this cannot. The study could be replicated with multiple coders who could bring more insights as this project could not do this. However, although concerning as researchers could be risking informant's safety due to the illegality of hacking, the interview and observations of newbies and hackers would yield a rich data set of understandings. For example, in their study of Wikipedia trolls, Shachaf and Hara (2010) conducted the study strictly by email to protect informants while Kubitschko (2015) sought data with permission from a major European hacking community becoming involved with them by attending their meetings. The ethics of doing any hacker research may be of interest to authorities; therefore, careful study design must be strictly adhered to in order to protect the researcher, informants and the institution or company they are researchers for.

To conclude, this study has given insights of newbies who face a formidable process to be accepted into the hacker community and earn titles more in keeping with what they want to achieve. The contribution to cyber crime prevention is in understanding the specific ways newbies operate in such environments. As the reach and frequency of cyber-attacks grows, perhaps with catastrophic results, such research which seeks to understand behaviors and motivations can support the practical security measures that governments and security firms are trying desperately to implement and deter newbies from entering the world of hacking.

References

Alhojailan, M. (2012). Thematic analysis: a critical review of its process and evaluation. *West East Journal of Social Sciences, 1*(1), 39-47.

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology, 4*(1-2), 643-656. Retrieved from http://www.cybercrimejournal.com/michaelbacchmaan2010ijcc.pdf.

Bourdieu, P. (1977). *Outline of a theory of practice*. (R. Nice, Trans.). New York: Cambridge University.

Bourdieu, P. (1984). *Distinction: a social critique of the judgement of taste*. London: Routledge.

Bourdieu, P. (1985). The social space and the genesis of groups. *Theory and Society*, *14*(6), 723-744.

Bourdieu, P. (1986). The forms of capital. In J. G. Richardson (Ed.), *Handbook of theory and research in the sociology of education* (pp.241-258). New York: Greenwald Press.

Bourdieu, P. (1990). *The logic of practice*. (R. Nice Trans.). Cambridge: Polity Press.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. http://dx.doi:10.1191/1478088706qp063oa.

Bruckman, A. (2002). *Ethical guidelines for research online*. Retrieved from http://www.cc.gatech.edu/~asb/ethics.

Chiesa, R., Ducci, S., & Ciappi, S. (2009). Profiling Hackers: *The science of criminal profiling as applied to the world of hacking*. Florida: Auerbach Publications.

Décary-Hétu, D., & Dupont, B. (2013). Reputation in a dark network of online criminals. *Global Crime, 14*(2-3), 175-196. doi: 10.1080/17440572.2013.801015.

Dremliuga, R. (2014). Subculture of Hackers in Russia. *Asian Social Science, 10*(18), 158-162.

Flowers, S. (2008). Harnessing the hackers: The emergence and exploitation of Outlaw Innovation. *Research Policy, 37*, 177-193. doi: 10.1016/j.respol.2007.10.006.

Fötinger, C., & Ziegler, W. (2004). *Understanding a Hacker's Mind – a psychological insight into the hijacking of identities*. Krems, Austria: Donau-Universität Krems. Retrieved from http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf.

Gottfredson, M. & Hirschi, T. (1990). *A general theory of crime*. Stanford, CA: Stanford University Press.

Hanks, W. (2005). Pierre Bourdieu and the practices of language. *Annual Review of Anthropology, 34*, 67-83. doi: 10.1146/annurev.anthro.33.070203.143907.

Holt, T., D., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology, 6*(1), 891- 903. Retrieved from http://cybercrimejournal.com/holtetal2012janijcc.pdf.

Imperva. (2012). Hacker intelligence initiative, monthly trend report 13: monitoring hacker forums ADC monthly web attacks analysis, October 2012. Retrieved from https://www.imperva.com/docs/HII_Monitoring_Hacker_Forums_2012.pdf.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *Sociological Review, 46*, 757-780.

Kao, D., Huang, F., & Wang, S. (2009). Persistence and desistance: examining the impact of re-integrative shaming to ethics in Taiwan juvenile hackers. *Computer Law and Security Review, 25*, 464-476. doi: 10.1016/j.clsr.2009.05.009.

Kilger, M., Stutzman., & Arkin, O. (2004). Profiling. In The Honeynet Project (2nd Ed.), *Know your enemy*. Addison Wesley Professional.

Kirwan, G., & Power, A. (2013). *Cybercrime: The psychology of online offenders*. Cambridge: Cambridge University Press.

Kollock, P. (1999). Invisible crowds in cyberspace: mapping the social structure of Usenet. In M. Smith & P. Kollock (Eds.), *Communities in cyberspace* (pp.195-219). London: Routledge.

Kshetri, N. (2010). The global cybercrime industry: Economic, institutional and strategic perspectives. Berlin: Springer.

Kubitschko, S. (2015). Hackers' media practices: demonstrating and articulating expertise as interlocking arrangements. *Convergence*: *The International Journal of Research into New Media Technologies, 21*(3), 388-402. doi: 10.1177/1354856515579847.

Madge, C. (2007). Developing a geographers' agenda for online research ethics. *Progress in Human Geography*. *31*(5), 654-674. doi: 10.1177/0309132507081496.

Mander, M. (1987). Bourdieu, the sociology of culture and cultural studies: a critique. *European Journal of Communication, 2*(4), 427-453. doi: 10.1177/0267323187002004044.

Markham, A., & Buchanan, E. (2012). Decision-making and internet research. Retrieved from http://aoir.org/reports/ethics2.pdf.

Meyer, G., & Thomas, J. (1990). The baudy world of the byte bandit: A postmodernist interpretation of the computer underground. In F. Schmalleger (Ed.), *Computers in criminal justice* (pp.31-67). Bristol (Indiana): Wyndham Hall.

Mitnick, K. (2002). The art of deception: Controlling the human element of security. Indianapolis: Wiley.

Nikitina, S. (2012). Hackers as tricksters of the digital age: creativity in hacker culture. The *Journal of Popular Culture, 45*(1), 133-152. doi: 10.1111/j.1540-5931.2011.00915x.

Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New Media and Society*, *6*(2), 195-217. doi: 10.1177/1461444804041445.

Pick, R. (2013). The "ethics" of teaching ethical hacking. *Journal of International Technology and Information Management, 22*(4), 67-75.

Schell, B., & Dodge, J. (2002). The Hacking of America: Who's Doing it, Why, and How. Westport, CT: Quorum Books.

Shachaf, P., & Hara, N. (2010). Beyond vandalism: Wikipedia trolls. *Journal of Information Science, 36*(3), 357-370. doi: 10.1177/0165551510365390.

Skågeby, J. (2015). Interpreting Online Discussions: Connecting Artifacts and Experiences in User Studies. *The Qualitative Report*, *20*(1), 115-129. Retrieved from http://nsuworks.nova.edu/tqr/vol20/iss1/9.

Taylor, P. (1999). *Hackers crime and the digital sublime*. London: Routledge.

Taylor, R., Fritsch, E., Liederbach, J., & Holt, T. (2011). *Digital crime and digital terrorism* (2nd ed.). Boston: Prentice Hall.

Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker. *International Journal of Cyber Criminology, 2*(2), 382–396. Retrieved from http://www.cybercrimejournal.com/Orlyijccdec2008.pdf.

Warren, M., & Leitch, S. (2009). Hacker Taggers: A new type of hackers. *Information Systems Frontiers, 12*(4), 425-431. http://dx.doi:10.1007/s10796-009-9203-y

Yar, M. (2005). Computer hacking: just another case of juvenile delinquency? *Howard Journal of Criminal Justice, 44*(4), 387-399. doi:10.1111/j.1468-2311.2005.00383.x.

Young, R., Zhang, L., & Prybutok, R, (2007). Hacking into the minds of hackers. *Information Systems Management, 24*(4), 281-287. doi:10.1080/10580530701585823.