ASPIRATION Journal Vol.2(1) July 2021, p.69-91
E-ISSN : 2723-1461

ASPIRATION Journal
(ASPIKOM Jabodetabek International Research of Communication)
Journal homepage: www.aspiration.id/index.php/asp

CYBERCRIME REPRESENTATION IN THE FILM "UNFRIENDED: DARK WEB"

Kenny Lee[1], Dewi Maria Herawati[2], Isiaka Zubair Aliagan[3]
[1,2] Universitas 17 Agustus 1945 Jakarta, Jln. Sunter Permai Raya, Sunter Agung Podomoro, North Jakarta, Jakarta, 14350, Indonesia
[3] Department Mass Communication, Kwara State University, P.M.B 4412, Irra Road, Offa, Kwara State, Malete Nigeria,
[1]kenkennylee97@gmail.com, [2]dewimaria86@yahoo.com, [3]isiakaliagan@yahoo.com

ARTICLE INFO

Received on March 26st, 2021
Received in revised from June 29 st, 2021
Accepted July 28th, 2021
Published on July 31th, 2021

Keywords:
Cybercrime
Representation
Semiotic
Darkweb

How to cite this article: Lee, Kenny; Herawati, D.M. & Aliagan, I.Z. (2021). Cybercrime Representation In The Film "Unfriend: Drak Web". *ASPIRATION Journal Vol.II(1), July 2021, p.69-91*

Copyright ©2020 The Author(s). Published by ASPIKOM Koordinator Wilayah JABODETABEK (ASPIKOM Regional Coordinators for Jakarta, Bogor, Depok, Tangerang and Bekasi) on behalf of the ASPIKOM Pusat (Association of Indonesian Communication Science Higher Education).
This is an open access article distributed under the terms of the Creative Commons Attribution-Non Commercial-No Derivatives License 4.0 (CCBY-NC-ND), where it is permissible to download and share the work provided it is properly cited. The work cannot be changed in any way or used commercially without permission from the ASPIRATION Journal.

ABSTRACT

This study aims to analyze cybercrime actions on dark web sites in the film Unfriended: Dark Web. This study seeks to reveal the 'form' of cybercrime contained in a dark web site linked in a film. By using John Fiske's semiotic analysis, this study makes effort to enlighten people's thinking through signs of reality, representations, and themed ideologies to be more careful in using the virtual world as a daily activity. The paradigm used in this study is the constructivism paradigm in forming a framework for understanding cybercrime acts in the object of this study. The methodology used is a Semiotic. The results of this study are films that are now being used for industrialization and commercialization. The results of this study also show the facts of reality, i.e., behavior, expressions, sounds, and so on. Then there is a representation that consists of technical codes in a film show, such as camera, lighting, editing, music, and sound as part of the description of the situation and storyline. Finally, there are elements of ideology, i.e., ideological codes, such as individualism, feminism, liberalism, capitalism, race, class, and materialism, which are in the film.

INTRODUCTION

Cybercrime is an act of crime by utilizing computers or computer networks to become tools, targets, or places for crimes perpetrated by individuals, groups or communities who violate the law and are also crimes that disrupt social balance or stability in people's lives.

Scanned with CamScanner

Cybercrime actions are carried out by utilizing the virtual world as a forum for committing crimes (Fuady, 2005).

Cybercrime perpetrated by a certain person or group can lead to the use of a Dark Web site, which is a dangerous dark web site and can threaten or even take someone's life if the perpetrator really has the intention of committing murder. This incident cannot be separated from the development of technologies that can be easily used by someone to do anything, including cybercrime. The Dark Web itself is a small part of the Deep Web, which is estimated to be around 400 to 500 times larger than the general internet where websites are not indexed so that they cannot be searched through search engines in public browsers (Supanto, 2016). Dark Web is also defined as site collections that allow users to be anonymous and undetectable. Daek Web can be imagined as a black market in cyberspace where there is no government control, and it is really a safe place for illegal activities. (Piliang, 2005).

The Dark Web is protected by encrypted mechanisms, e.g., "TOR" (The Onion Router), where users can protect their privacy rights such as their identity and geographic location while browsing for information. The TOR itself was built with the assistance of funds from the United States Government, especially from the Ministry of Defense, to create a free flow of communication for the public in areas where the internet is prohibited from gaining access to information or providing information to the foreign nations (Gollese, 2006).

Everything has its pros and cons. This also applies to Dark Web as part of the internet that is completely untraceable or even penetrated is a favorite place for pornographers, sex dealers, drug dealers, terrorists and thieves who sell hacked Social Security and credit card trading. In 2013 alone, Dark Web also contained more than the identity sales of 40 million credit/debit cards hacked during Black Friday events at Target stores (Zuraida, 2015). Of the 2 million Dark Web users, Indonesia is in the top five largest user base along with Russia, the United States, Iran, and Turkey.

The film "Unfriended: Dark Web" is one of the films that depicts the dark side of cyberspace and Cybercrime activity. The film was directed and the script was written by Stephen Susco. "Unfriended: Dark Web" tells the story of a group of teenagers who found a laptop. Unexpectedly, the laptop had access to a 'Dark Web' site or a forbidden page and the group of teenagers did not know that the laptop had a camera connected to the hackers' laptop. The film was first released at the South by Southwest festival on March 9, 2018. Then, on July 20, 2020, the film was distributed in theaters in the U.S. by Universal Pictures' OTL

Scanned with CamScanner

Releasing and Blumhouse Producions. This film managed to get good response from the audience to make a profit of 16 million US dollars, even though the budget prepared for this film is only 1 million US dollars. Unfriended: Dark Web has a duration of 1 hour 32 minutes and received a rating of 5.6/10 from IMDb.com (IMDb 2018).

After knowing the meaning of the Dark Web that leads to cybercrime action through the use of cyberspace, the writer wants to explore the reality, representation, and ideology of Cybercrime in the film "Unfriended: Dark Web". Through this research, every sign that indicates cybercrime actions on the Dark Web site will be interpreted using the three elements of John Fiske's analysis, i.e., reality, representation, and ideology.

Based on the existing research background, the researcher made effort to formulate the occurring problems. The formulation of the problem from the background of the study is, How is the Representation of Cybercrime in Unfriended: Dark Web Film? This research is conducted to analyze the reality, representation, and ideology that appear in the film "Unfriended: Dark Web".

CONCEPTUAL FRAMEWORK

Previous studies were made as a reference for how well the researcher understands the research they were doing, i.e., by presenting several references from previous studies which of course have a relationship to the theme or topic of the research. For more details, the following are some of the previous studies reviewed by the researcher:

Carreta, Tjahyana. and Budiana's (2019) study explored the reality, representation, and ideology of cybercrime contained in the film "Searching". Their study used representation theory with John Fiske's semiotic analysis. Their findings in the film "Searching" are the creation of Post-Truth in the form of fake news, hoaxes (twisted factual news) (Lusi, 2019), then the discovery of security issues of identity, cyberbullying, and data interpretation. Previous and ongoing studies show the same theory used, i.e., John Fiske's theory of representation.

Furthermore, Wilona (2015) explored the reality, representation, and ideology of crime contained in the films "Ted" and "Ted 2". Their study used representation theory with John Fiske's semiotic analysis. The results of their study show that the films "Ted" and "Ted 2" both represent the existence of criminal acts that include various elements of drug use, the holding of sharp weapons/fires, physical violence, assault, and destruction of other people's

Scanned with CamScanner

property. Previous and ongoing studies show the same theory used, i.e., John Fiske's theory of representation.

In this study, the researcher used a constructivist paradigm to explore reality, representation, and ideology in the form of Cybercrime in Unfriended: Dark Web. By using representation theory, the researcher makes effort to analyze cybercrime actions contained in the Dark Web site that are often experienced by someone when accessing cyberspace. The analytical method used by the researcher is John Fiske's semiotic analysis for the process of peeling off signs in the form of representation, reality, and ideology regarding Cybercrime on the Dark Web site and to find cybercrime actions on the Dark Web site in the film. The following section below is a framework used in this study.

John Fiske's Theory of Semiotics

Semiotics is a branch of science about signs which has specific and standard principles, systems, and rules. Semiotics is different from natural science which has the nature of certainty, objectivity, and unification. This is because semiotics is built to be more open to various interpretations. As a branch of science that has a broad scope of study and covers almost all fields of life, it has resulted in the creation of special semiotics, i.e., art semiotics, medical semiotics, animal semiotics, architectural semiotics, fashion semiotics, film semiotics, literary semiotics, and television semiotics. (Mudjiono 2011)

Semiotics helps to interpret various communication signs, both natural and artificial signs, semiotics is able to interpret the meanings both implied and express, because basically semiotics is based on the logic or subjectivity of the interpreter itself. This is what gives rise to several streams of semiotics, such as the flow of semiotics structuralism, pragmatism, post-modernism, and its differentiator is subjectivity based on epistemology, ontology, axiology, and methodology. Signs that exist in semiotics usually consist of natural signs, i.e., signs that occur naturally, and conventional signs, which are signs specially made for communication. John Fiske's semiotics follows the flow of post-structuralism, this flow was born because of disagreement with the flow of structuralism pioneered by Ferdinand De Saussure which said that signs in semiotics are binding, and do not give the possibility of creating new signs of creativity and the flow of post-structuralism. John Fiske's semiotics does not reject all forms of attachment to new conventions, rules or codes, but opens space for creative, productive, subversive, transformative, sometimes anarchist models of language and signaling (Piliang, 2010:259).

Scanned with CamScanner

John Fiske in the book Culture and Communication studies, states that communication is talking to one another. At this level, communication can be understood in the context of messages conveyed via television, as the dissemination of information; or it could be in the form of nonverbal communication such as hairstyles or literary criticism. (Fiske 2010). John Fiske assumes that all communication involves signs and codes. A sign is an artifact or action that refers to something other than the sign itself. Signs denote constructs, and code is the system by which signs are organized and that determines how they may relate to one another. Another assumption is that signs and codes are transmitted or made available to others and that acceptance of signs/codes/communications is a social relationship practice.

In Fiske's view, an event in a television show will become a television event if it has been encoded by social codes, which are constructed in three stages (Utomo, Jupriono, & Ayodya 2018) as follows:

1. Reality

In the reality stage, television shows present the reality of events in appearance of clothing, environment, behavior, conversation, gestures, expressions, sounds, and so on. In a sense, all forms of television shows really show something real or according to facts that exist in the midst of society. For example, if you are reporting a tsunami event, a news broadcast must display a picture of the moment the tsunami hit the shore, tsunami impacts, houses that were affected by the tsunami, and so on.

2. Representation

The act of presenting something through something other than itself, usually in the form of a sign or symbol. The representation in television shows is related to technical codes, such as cameras, lighting, editing, music, and sound. These elements are then transmitted into representational codes that can actualize reality in television shows.

3. Ideology

Belief systems and value systems represented in various media and social actions. In this stage, all elements are organized and categorized in ideological codes, such as patriarchy, individualism, race, class, materialism, capitalism and so on.

Scanned with CamScanner

METHODOLOGY

The researcher made effort to explain the right paradigm for the research that will be carried out, i.e. to explore the reality, representation, and ideology related to the film Unfriended: Dark Web. In this study, the paradigm used is the constructivism paradigm.

The constructivism paradigm is almost the antithesis of an understanding that places observation and objectivity in discovering a reality or science. This paradigm views social science as a systematic analysis of socially meaningful action through direct and detailed observation of the social actors concerned creating and maintaining/managing their social world (Hidayat 2003).

According to Patton, constructivist researchers study a variety of realities constructed by individuals and the implications of these constructs for their lives with others. In constructivism, each individual has a unique experience. Thus, a research with this paradigm suggests that every way that individuals take in seeing the world is valid, and there needs to be a sense of respect for this view (Patton, 2002). The constructivism paradigm sees reality as something that exists, but reality is plural, and its meaning is different for each person.

According to the constructivist paradigm, the social reality that is observed by a person cannot be generalized to all people whom positivists usually do. The constructivism paradigm traced from Weber's thought assesses human behavior as fundamentally different from natural behavior, because humans act as constructing agents in their social reality, both through giving meaning and understanding behavior among themselves. This constructivist paradigm study places the position of the researcher as equal and as much as possible to enter with the subject, and tries to understand and construct something that becomes the understanding of the subject to be studied. Constructivism theory states that individuals interpret and act according to conceptual categories of thoughts. Reality does not describe the individual but must be filtered through the way people perceive that reality.

The purpose of using the constructivism paradigm in this study is to observe and place objectivity in finding a reality from the contents of a film, i.e., the film "Unfriended: Dark Web". In this study, the researcher tried to peel or reveal the contents of the film in the form of signs such as reality, representations, and ideology of Cybercrime on the Dark Web site in the film "Unfriended: Dark Web".

Scanned with CamScanner

Conceptual Foundation; Cybercrime and the Dark Web

Criminal activities can be carried out anywhere and anytime, including in cyberspace. Someone who commits criminal activities in cyberspace usually uses dark sites as a medium for operating such as Dark Web sites. The two certainly have different meanings but can be related to each other, Cybercrime itself is a criminal activity using computers or computer networks to become a tool, target or place of crime, including cybercrime. In addition, Dark Web refers to encrypted online content that is not indexed by conventional search engines.

Cybercrime is a new phenomenon in crime as a direct result of the development of information technology. Several names are given to this new type of crime in various writings, including "cybercrime" (cyberspace/virtual-space offence). It is also a new dimension of "hi-tech crime", a new dimension of "transnational crime", and a new dimension of "white collar crime & blue-collar crime" (Arief, 2006). In law, Indonesia also has a special law regarding cybercrime, i.e., the 2008 ITE law, which discusses procedures, limitations on computer use, and the sanctions that will be given if there is a violation.

Cybercrime is basically a crime related to information. The information system itself, as well as a communication system which is a means of conveying/exchanging information to other parties (transmitter/originator to recipient) according to Sutanto in his book on Cybercrime-motive and Cybercrime prosecution consists of two types, i.e.:

1. Crimes using information technology (IT) as a facility. Examples of this first type of cybercrime activity are piracy (copyright or intellectual copyright, etc.); pornography; credit card fraud and theft (carding); fraud by e-mail; fraud and bank account break-ins; online gambling; terrorism; perverted site; race and religion hate-related internet materials (such as the spread of ethnic and racial or religious hatred); transaction and distribution of illegal drugs; sex transactions; and others.

2. Crimes that target information technology (IT) systems and facilities. Cybercrime of this type does not use computers and the internet as a medium or means of criminal acts, but rather makes it a target. Examples of the types of crimes include illegal access to a system (hacking), destruction of internet sites and data servers (cracking), and defecting.

Cybercrime qualifications, as in Barda Nawawi Arief's book, according to the 2001 convention on cybercrime in Budapest Hungary, are as follows:

Scanned with CamScanner

1. Legal interception: i.e., deliberately and without the right to hear or capture secretly the transmission and transmission of non-public computer data to, from, or within a computer system using assistive devices.

2. Data interference: committed intentionally and without right to destroy, delete, or change computer data.

3. System interference: i.e., deliberately making interference or serious obstacles without right to the functioning of the computer system.

4. Misuse of devices: misuse of computer equipment, including computer programs, computer passwords, access codes.

5. Computer related forgery: forgery (intentionally and without the right to enter change, delete authentic data to be inauthentic with the intention of being used as authentic data)

6. Computer related fraud: fraud (intentionally and without rights causing the loss of property of others by entering, changing, deleting computer data or by interfering with the functioning of the computer/computer system, with the aim of obtaining economic benefits for himself or others);

7. Content-related offenses: offenses related to child pornography;

8. Offences related to infringements of copyright and related rights: offenses related to copyright infringement

Research Methods

In this study, in order to explore every sign of Cybercrime in the film "Unfriended: Dark Web", the researcher used descriptive research with a qualitative approach. The descriptive method is fact finding with the correct interpretation. Descriptive research studies problems in society, as well as the procedures that apply in society and certain situations, including the relationship between activities, attitudes, views, ongoing processes and the influence of a phenomenon. Descriptive research is a research method that seeks to describe the object or subject under study in accordance with what it is.

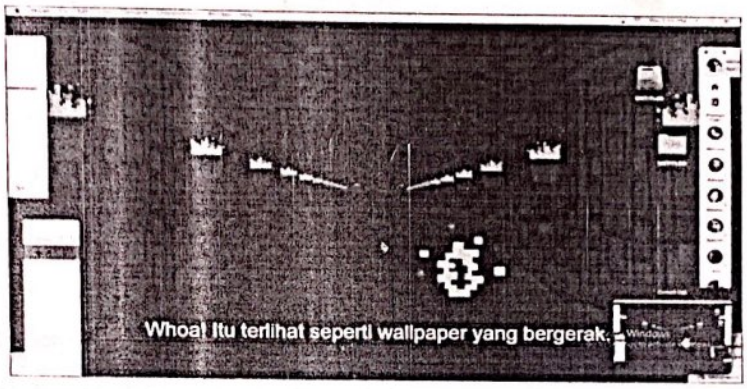
FINDINGS & DISCUSSION

Analysis of Reality, Representation, and Ideology

Scanned with CamScanner

The analysis in this study is by showing the scenes taken from the film Unfriended: Dark Web, where in each scene the author described further with the theory of John Fiske, i.e., regarding the reality, representation, and ideology of the film that the author adopts. The following are the results of the analysis by the author:

Figure 1. Views of the Dark Web film Unfriended: Dark Web, Duration (00.28: 36-00.28: 37)

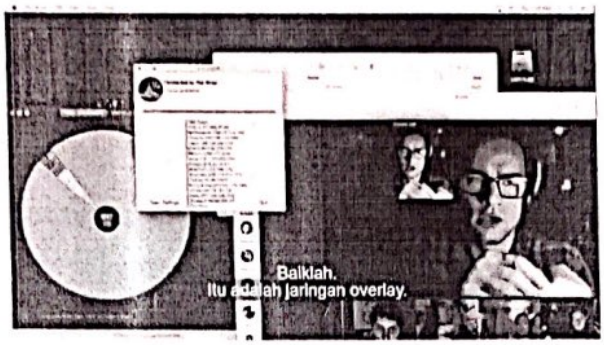


In scene 1 above, Matias shows the appearance of "The River" on the laptop he found at a café. According to www.unfriended.fandom.com, "The River" is the name of the BBS (Bulletin-board system) used by a very strong and large organization of sophisticated, sick-minded hackers, and also the antagonists in the film Unfriended: Dark Web. In addition, the scene also shows a conversation from AJ who is Matias' friend, where in the conversation it is seen that AJ is very surprised by saying "Whoa! It looks like a moving wallpaper". According to the theoretical understanding of John Fiske, it can be interpreted that AJ's conversation shows an element of reality in it because the conversation is part of John Fiske and the conversation also shows the impression of being surprised which is part of the expression when speaking.

Next is the element of representation. The scene contains elements of representation that can be measured from the film's technical codes. The form of technical codes in the first scene can be seen from the way the scene is taken in the film using a computer screen as a point of view in taking the scene. Then there is a small computer screen located in the lower right corner that shows that you are doing a video conference.

Scanned with CamScanner

Figure 2. Damon explains another meaning of "The River", Duration (00.28: 45-00.28: 46)



In scene 2 it explains that Damon, who is wearing glasses and wearing earphones, is explaining to Matias, AJ, Nari, Serena, and also Lexx through a video conference about what Matias shows through his laptop which he found at a cafe, precisely when Matias took the laptop as a "safekeeping". Matias did have the desire to have a new laptop, so he decided to take a laptop belonging to someone he didn't know from the "deposit box". Then, when he used the laptop, it turned out that he found a program called "The River" which they had no knowledge about. Then, Matias decided to ask Damon about the program, and Damon said "Okay. It is an overlay network, it is a part of the internet that does not exist or cannot be indexed by search engines."

An overlay network is a series of virtual or physical computers layered on top of the existing network. The purpose of an overlay network is to add lost functionality without a complete network redesign. Common examples of overlay networks are found in cloud computing structures and peer-to-peer networks. Peer-to-Peer Networks just as the Internet uses telephone lines as a backbone, peer-to-peer networks use standard Internet protocols to prioritize data transmission between two or more remote computers. Peer-to-peer is a type of overlay network, because it uses a special software-based application (Elis Maulidiyah, 2015). In other words, an overlay network is a part of the internet that does not exist or cannot be indexed by search engines.

When Damon explained about the overlay network, AJ showed an expression that was resting his chin using his left hand with a gaze that showed that he was listening carefully to what Damon was talking about. Just like AJ, Matias, Serena, Nari, and Lexx also showed expressions with their two very serious eyes by looking at the laptop while listening to Damon's explanation regarding the overlay network. It can be concluded that AJ, Matias,

Scanned with CamScanner

Damon, Serena, Nari, and Lexx show gestures and expressions as forms of reality which are part of John Fiske's theory.

The representation in the second scene above can be seen when they do a video conference by taking a medium shoot so that it looks close to a camera. Because they conducted a video conference using a computer screen as a form of perspective in the film, it was clear that there were two different types of lighting in the room, the first was the Damon and Lexx rooms showing slightly dark lighting and then for Matias, AJ, Serena, and Nari showed bright lighting in their respective rooms.

Figure 3. AJ summed up Darknet, Duration (00.28: 59-00.29: 00)



In scene 3 above, AJ concludes that what Damon said about the overlay network is the darknet or also known as the dark web. AJ's gesture show that he was overjoyed after learning that the overlay network Damon described was actually a dark web site. Ekman (2003) explains that happy emotions are often associated with the appearance of a smile on the face, and this can be seen clearly on AJ's face, where both his eyes and eyebrows are seen to rise, then his hands are raised again, and AJ's mouth is slightly wide open, which shows that AJ has a shape of happy emotions and it is a form of emotion that is positive in nature.

In contrast to the expressions on Matias and Serena's faces, the two of them were seen scratching their respective heads with one hand which showed that they were confused by what AJ said about the dark web. Hands scratching their neck or head can mean that the person is thinking or trying to find the right words to say. If this hand movement continues in

Scanned with CamScanner

a conversation, we can guess that the person is nervous and has difficulty expressing their feelings (Kompasiana, 2012).

After talking about facial expressions that are part of John Fiske's theory of reality, the next is in terms of clothing and environment from Matias, Damon, AJ, Serena, Nari, and also Lexx. In terms of clothing, AJ wears a green shirt with black stripes with a white collar that looks very relaxed according to AJ's environment, i.e., being in the house, right in the living room. The same is the case with Serena and Nari, where their surroundings are in a large enough room which shows that both of them are in the living room as well as the terrace and table in the room.

However, Matias, Damon, and also Lexx, the three of them are in a room that is not too large, which describes being in a bedroom respectively. Matias, who is wearing a plain blue shirt, is in a room that is not too large, plus a bicycle is hanging and there is a sofa behind Matias. For Damon, he wears a brown city-check shirt and around it is a blue light which appears from the computer hardware connected to his computer. The environment is not too wide and illustrates that Damon is in his bedroom. Meanwhile, Lexx was wearing a black leather jacket and dark t-shirt, while using earphones like Damon. Similar to Damon, behind Lexx there is also a laptop and a computer desk that shows that Lexx is in his bedroom.

Figure 4. AJ and Serena fear, Duration (00.32: 15-00.32: 16)



Scanned with CamScanner

Next, Scene 4, in this scene there are several elements of reality that can be implemented in John Fiske's theory. The first was a gesture from AJ who was holding his head with both hands after knowing that a hacker could break into the camera on a laptop. In addition, AJ also covered his ears and bowed his head when he found out that a hacker could do this. The gesture performed by AJ reflects that he does not expect and is also afraid that hackers can break into the camera on a laptop. Then Serena's gesture revealed that she was terrified after knowing this. This can be seen from her facial expression, starting from her two eyes that are slightly closed as if to mean that her expression is afraid and then her mouth is slightly raised plus the right hand that holds her chin, which is very clear that Serena is afraid of the hacker's behavior.

Meanwhile, according to the Oxford English Dictionary, fear is a state of the soul which is marked by an understanding or image that our physical integrity or some other organ of equal value to us is in a dangerous state. Goleman (in Manizar, 2016) classifies the emotions of fear into several following categories:

1. Being Anxious

Anxiety is a special situation that is unsatisfactory and unpleasant with the power to release these feelings in certain ways

2. Feeling Worry

Worry is a cognitive aspect of anxiety experienced in the form of negative thoughts about themselves and their environment and negative feelings about the possibility of failure and its consequences

3. Being Alert

Alert is to be careful and watchful; or get ready

4. Horrified

Horrified is feeling afraid or worried because of seeing something scary or experiencing a dangerous situation

5. Panic

Panic is a period that increases fear and discomfort that is strong and fast accompanied by physical symptoms such as a fast heartbeat, trembling, shortness of breath, dizziness, or nausea

According to Hude (in Aditya, 2015: 101-102), expressions of fear are characterized by the following changes in behavior: pale face, lowering one's head, covering ones ears,

Scanned with CamScanner

avoidance, shouting hysterically, and blurred eyesight. Apart from the reality element, there is also an ideological element in scene 4. This scene 4 contains elements of liberalism ideology, because there is an element of freedom for each group to be able to express their own desires without any restrictions from other parties. This ideology assumes that everyone should have the same opportunity to achieve something. In addition, what hackers do is to express their own desire to achieve something. Of course this contains elements of the ideology of liberalism, with prevention from other parties allowing hackers to carry out various forms of action that can harm a country and nation.

Figure 5. Matias being terrorized by Hackers, Duration (00.35: 29-00.35: 30)



Scene 5 above contains an element of John Fiske's reality in the form of a conversation that Matias has with Hackers via private chat from a program "The River" that has been opened by Matias. The following is the content of the conversation that the author has translated:

Charon IV = "*Right*"
Charon 68 = "*Is that enough?*"
Charon IV = "*For what?*"
Charon 68 = "*Paint is darker. Black. Leave it long and straight. And method different. Which is slower.*"
Charon IV = "*What method*?"
Charon 68 = "*Trephination (Trepanasi), "the procedure to drill a hole in the skull*".
Charon 68 = "*Then put something inside*"
Charon 68 = "*Show him. I want to see his eyes*".
Charon 68 = "*Use a mirror. I want him to see too*".
Charon 68 = "*I would pay more if it was a living being*".
Charon 68 = "*And if he is alive then enter*"

Scanned with CamScanner

Figure 6. Files traded by Hackers, Duration (00.38:01-00.38:02)



After knowing the contents of Matias' conversation with the hacker, Matias was warned by AJ, Damon, Serena, Lexx, and also Nari to turn off the private chat that was being used in a high voice, they said, "Matias, turn it off!". As for Matias' 'sad' facial expression, this can be seen from Matias' eyes that wanted to cry and also the shape of Matias' eyebrows that pointed downward, illustrating that he did not expect what the hacker said to Matias via private chat. Private chat itself is a private chat room that cannot be known by other people and is very confidential in nature. Usually, a hacker always uses a private chat room to carry out their actions by providing a form of threat to the victim for an advantage.

In scene 6, there is an element of reality through conversations conducted by AJ. AJ said "That's what they are trading", which is why Matias was told by the hacker to open a folder called "Contributions". Matias finally opened the folder then played the contents of the video and it turned out that the video was a collection of crimes against women, such as kidnapping, and also assault and there was a break-in of cctv recordings from various places by hackers when carrying out the action. The hacker was targeting a girl to be used as their next action and it turned out that the hacker was paid by someone and made a profit.

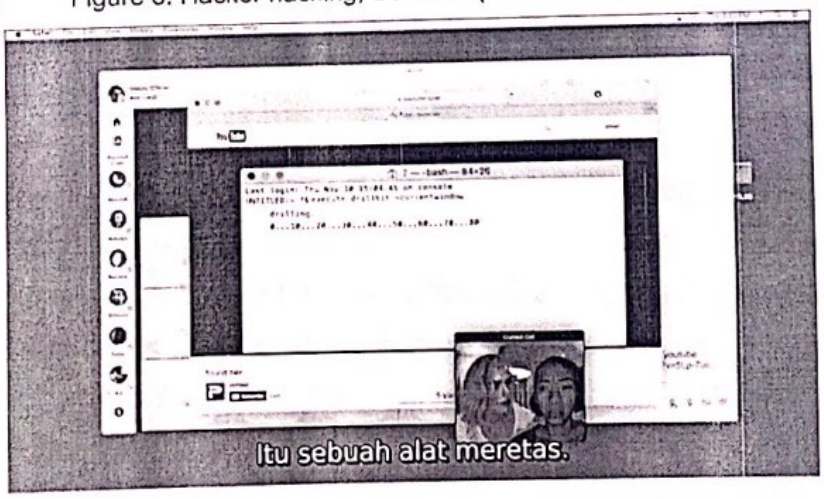
Scanned with CamScanner

Figure 7. Hacker breaking into skype, Duration (00.59:04-00.59:05)



After knowing the contents of the video, the ideology contained in this scene is adhering to the ideology of feminism. This ideology emphasizes the equal rights and obligations of women. This equality includes economic, political, social, cultural, personal and public sphere rights. The main goal of this ideology is to fight for women's rights from various factors.

Figure 8. Hacker hacking, Duration (00.59:47-00.59:48)



Then for scene 7, Serena, who was holding Nari's shoulder, said "Matias? Get rid of him", Serena's voice sounded panicked. Matias' expression was also very confused when he saw that the hacker was able to enter a video conference chat which was being held by Matias and his friends. This confused expression could be seen in Matias' eyes, which were filled with blank stares when he saw the hacker's action. Not only Matias, Serena, Nari, and AJ

Scanned with CamScanner

also have the same expression as Matias. This is in contrast to Damon who looks calm when he witnesses the hacker's action. Damon whose gesture of both hands was under his chin described that he looked calm and showed curiosity with Damon's eyes. AJ looked very tense, he immediately straightened his body when he saw the hacker's action, as if AJ could not deny that hackers could actually do forbidden acts.

Finally, in scene 8, Serena stares at Nari with a confused expression when she sees the hacker hacking with a program called "Drillbit Hacking Tool". Nari also looked confused when she saw the program moving on its own, this could be seen with her slightly open mouth gesture which illustrated that she was surprised by what the hacker was doing. After knowing what the hacker was doing, Damon said, "It's a hacking tool". It turns out that what Damon said made Serena and Nari both shocked and confused. Drill bit hacking tool is a program that can crack passwords on social media accounts or other applications in a short time.

In addition to gestures and expressions, the author wants to discuss the clothes worn by Serena and Nari. Both of them were wearing t-shirts, Serena was wearing a white t-shirt, while Nari was wearing a red t-shirt, and both of them showed that they were inside the house because behind them there was a lamp stand that was lit very brightly.

Data Interpretation

In this case, the author explains what causes cybercrime:

1. Cybercrime is carried out because of financial problems

Cybercrime is often committed by hackers, one of which is because of financial problems and the actions that hackers usually take are carding. Carding is credit card fraud performed by a perpetrator who knows that a person's credit card number is still valid, then the perpetrator can buy goods online whose bill is addressed to the original owner of the credit card. The perpetrator is called a carder. Another term for this type of crime is cyberfraud, aka fraud in cyberspace. Carding crimes have two scopes, national and transnational. Nationally, carding actors do so within the scope of one country. Transnational is when the carding actor crosses national borders.

Apart from carding, in the film Unfriended: Dark Web, a hacker commits a crime by breaking into the victim's laptop which then contains a dark web program whose contents are a collection of forbidden videos (containing elements of violence). After the hacker manages to break into the laptop and finds out about the contents of the laptop, it turns out that a dark web program is found and then a violent video is found, then the hacker can make a threat to the owner of the laptop to distribute the video if the laptop owner does not give some money.

Scanned with CamScanner

2. Cybercrime is carried out because of problems related to political, military, and nationalist sentiments.

For cases like this, usually a hacker has a personality that can be said to have no spirit of nationalism towards their own country or hates their own country because of political factors that are unfair to the people. Therefore, hackers also commit crimes by breaking into political and military systems in a country to break the national unity by committing cyber terrorism. Cyber terrorism is the use of computer network equipment to disrupt the country's infrastructure system (energy, transportation, government operations, and the like) or to intimidate the government or a group of civilians.

One of the most well-known terrorist groups in the world is Al-Qaeda. Terrorists used the Internet prior to the events of September 11, 2001. The Internet media is known as a very powerful tool for terrorist organizations. Prior to 1999, nearly 30 terrorist groups were discovered on the Internet by the United States Department of Government (Banez, 2010: 16). However, the role of the Internet was even stronger for them after the events of 9/11, as the Al-Qaeda leadership tried to distribute videos of their hiding in Pakistan via Al-Jazeera television, but they were frustrated with their very small segment that the message could be misunderstood. This then makes them turn to the Internet to upload it in a clearer and more detailed way without any editing (Gardner, 2013).

3. Cybercrime is carried out because of the perpetrator's satisfaction factor; there are psychological problems from the perpetrator.

Cybercrime behavior is described by Rogers (2010) through categories in the form of a taxonomic continuum ranging from new people (novice) and amateurs in the form of ordinary delinquency to major acts of terrorism (Sarinastiti and Vardhani 2018). The categories are as follows:

a. Script Kiddies (SK), are individuals with limited technical abilities, without really understanding what the impact of their behavior is. The main factors of this category are immaturity, increased ego and sensation seeking or adrenaline effect, having an underdeveloped sense of morality (can be seen from the Kohlberg morality scale—naïve instrumental hedonism). The obvious characteristic is that they often brag or show off their exploits, seek attention, and attack the ego of the other party.

b. Cyber-punks (CP), i.e., groups that "expand" the punk mentality into cyberspace. This group has no respect and no care for authority, symbols, and social norms. The main drive

Scanned with CamScanner

for their behavior is the need for recognition or fame from their peers and society. The demographics of this category are dominated by males aged 12 to 18 years. Fear is not a barrier, because the status of having been arrested or getting caught more often makes them proud. This is synonymous with a badge of honor and can raise their reputation as an underground folk hero.

c. Hacktivist (H), which is a term used for individuals or groups who perform deviant behavior, but with semantic camouflage to disguise their actions. Perpetrators tend to justify their destructive behavior with the label "public disobedience" and political and moral justifications for their behavior. Empirical data show that political motivation is a less decisive force. More basic motives are revenge, power, greed, marketing or media attention.

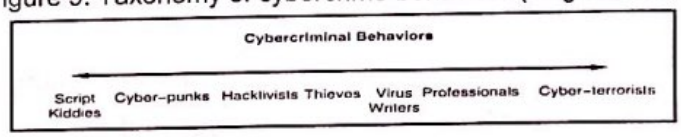
d. Thieves (T) is a criminal in general. His main motivations are financial gain and greed. The targets of this category group attack are usually credit cards and bank accounts, i.e., bank transfer fraud and misuse of credit card numbers. Parallel to this theft crime is identity theft.

e. Virus Writers (VW), starting from adolescence and developing into a category of ex-writers in line with their cognitive and chronological development and maturity. There is a sensation of mental challenges and academic practice (learning) in the viral process. Academic/intellectual training regarding the consequences of the virus it creates usually occurs after the virus has spread.

f. Professional (P) is the most elite category group in cyber criminals, who have competitive intelligence and gray activity. These P individuals can engage in high-profile scams to corporate espionage. They will sell information and intellectual property to the highest bidder.

g. Cyber-terrorists (CT) can be part of the military or paramilitary of a country and are positioned as soldiers or vice versa as fighters for liberation in the cyber battlefield. Their goal is the same as in traditional military, which is to win battles or wars. CT carries out two functions, i.e., attacking the enemy's defense system and society and protecting its own system from similar attacks from the opposing side.

Figure 9. Taxonomy of cybercrime behaviors (Rogers, 2010)



Scanned with CamScanner

Someone can be interested in committing cybercrime in a simple way that can be understood from the basic motivation as the author has explained one by one in each category of perpetrator. Cybercrime behavior can be further explained theoretically through social learning theory, moral disengagement theory, and anonymity as explained by Rogers (2010):

a. Social Learning Theory

The social learning process works in the context of social structures, interactions and situations. Criminal behavior is a function of the variables of the social learning process, especially reinforcement. The main mechanisms in social learning include differential reinforcement and imitation. Definitions in one's social environment are achieved by imitation and observational learning. Reinforcement can be in the form of tangible and intangible rewards in the form of the activity itself, money, or social rewards including increased status in social interactions. Over time, imitation is no longer important because what determines the next behavior is the reinforcement or the consequences.

Cybercrime perpetrators associate with other actors who have similar opinions on ethics and morality regarding deviant behavior. For cybercrime actors, computer mediated communication (CMC) is as important as relationships by ordinary people. Previously, many studies revealed interesting things about cybercrime perpetrators, such as a lack of social skills such as communication and face-to-face interaction. However, later research further revealed that on the other hand, principals had higher CMC-based social skills, i.e., "netiquettes", than people who were not or less familiar with CMC.

CMC allows its users to interact with one another and creates an environment where reinforcement and punishment can be made. Positive reinforcement will increase the tendency for involvement and vice versa. Positive reinforcement is in the form of praise, encouragement, and the achievement of folk hero status in the community. Punishment is in the form of isolation, ignorance, closing the flow of information, and locking specific channels. Reinforcement from the real world is when an action gets the attention of the media or society and others, and vice versa, when it does not get attention or appreciation from the community regarding the action.

b. Moral Disengagement - moral justification

Cybercriminals are generally described as modern Robin Hoods, who carry valuable functions in society. Many articles, editorials and interviews and web pages claim that without hackers, there would be no "real" security in cyberspace. The hackers interviewed by media

Scanned with CamScanner

argued that they acted as society's "watchdogs", maintaining a "watchful eye" on unscrupulous vendors and tyrannical governments. Unfortunately, many people accept the surface value of cybercrime.

Cybercrime behavior feels the need to justify their deviant actions. This is understandable because humans do not usually engage in a despicable act unless they succeed in convincing themselves that their actions are right. The process of moral justification makes destructive behavior personally and socially acceptable by depicting the act as a valuable social work, or fulfilling a higher moral purpose. This complex process can be understood through Albert Bandura's social cognitive theory and the concept of moral disengagement. Based on social cognitive theory, humans tend to naturally refrain from behavior that violates their moral standards and have feelings of guilt and self-criticism (self-censure) (Abdullah 2019). Moral standards are obtained from moral agency and manifested in the self-regulation mechanism, which consists of three things, i.e., self-monitoring, judgment (judgmental), and self-reaction (self-reactive).

According to Bandura's theory, one can infiltrate the self-regulatory system by separating internal moral control from destructive behavior through four mechanisms, i.e:

1) Reconstruct the behavior (through language and labels, etc.);
2) Disguise personal causal agents or distort behavior with its consequences. Cassidy, Faucher, and Jackson (2013) explain that the cyber world makes users detach from emotional contact and results in deindividuation. This in turn results in the interruption or dullness of the empathic response that results from the pain being exerted;
3) Misrepresenting or confusing the negative consequences of their behavior;
4) Vilify or blame or demean the victim.

c. Anonymity and Social Control Theory

Cybercrime behavior can be explained through social control theory related to anonymity. This theory states that a person refrains from criminal or deviant behavior because of social controls, including norms of decency, law, police, etc. When control is lost, deviant behavior will increase. In the real world, individual behavior is moderated by social identity which is part of social norms and cultural morals, so that behavior is more conservative and in line with existing social tolerances.

Research on online behavior has found that people behave differently in cyberspace than in the real world. Individuals tend to be more aggressive, less tolerant, more indiscriminate, and their opinions tend to be more polarized to extreme points on the continuum. The researcher

Scanned with CamScanner

hypothesize that anonymity tends to bring out the worst in individuals when they are online, because they believe that they are anonymous.and can pretend to be undercover personas. In simple terms we can understand that online behavior reflects the actual individual self in conditions without self-control and without social norms or pressure.

CONCLUSION

The purpose of this study is to explore the reality, representation, ideology in the film "Unfriended: Dark Web". Thus, every cybercrime action were described through this study. In the data analysis process, the researcher used John Fiske's semiotic analysis model. In the use of John Fiske's semiotic analysis, the researcher classifies every cybercrime incident into three orders or three stages of analysis, i.e., reality, representation, and ideology. The results of the analysis obtained show that the researcher knows the elements of reality, which consists of appearance of clothes, environment, behavior, conversation, gestures, expressions, sounds, and so on. Then, the researcher also knows the elements of the representation which consists of technical codes in a film show, such as camera, lighting, editing, music, and sound. And finally, the author also knows the elements of ideology, i.e., ideological codes, such as patriarchy, individualism, feminism, liberalism, capitalism, race, class, and materialism.

LIMITATION AND STUDY FORWARD

The suggestions from this research are aimed at filmmakers, presumably in the making of the film Unfriended: Dark Web, it displays a scene that discusses the causes of a hacker to commit cybercrime on a dark web site. This is because the people watching can understand the story behind the emergence of cybercrimes committed by hackers. When the audience knows the cause, surely the public will be more aware of the social media they have and will not commit any illegal actions, because if a certain group commits a crime that violates the law it could potentially be hacked by an irresponsible individual and could potentially also be disseminated in cyberspace.

Therefore, it is better for these filmmakers to be more detailed in explaining the meaning of a hacker who commits cybercrime on a dark web site. The researcher is also very aware that this research is still far from perfect, but the researcher will try to perfect this study in the future by analyzing each scene to make it more critical by using John Fiske's semiotic theory.

Scanned with CamScanner

REFERENCES

Abdullah, S. M. (2019). Social Cognitive Theory: A Bandura Thought Review published in 1982-2012. Journal PSIKODIMENSIA Volume 18, No. 1, 2019: 85-100.

Ali,I. (2012). Kejahatan Terhadap Informasi (cybercrime) dalam Konteks Perpustakaan Digital. VISI PUSTAKA Vol. 14, No. 1, 2012: 32-38.

Arief, B. N. (2006) Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia. Jakarta: PT Raja Grafindo Persada.

Fiske, J. (2010). Cultural and Communication Studies: Sebuah Pengantar Paling Komprehensif. Yogyakarta: Jala Sutra.

Fuady, M.E. (2005). Cybercrime: Fenomena Kejahatan melalui Internet di Indonesia. MEDIATOR Vol. 6 No.2, 2005.

Gollese, P.R. (2006) Perkembangan Cybercrime dan Upaya Penanganannya Di Indonesia oleh POLRI. Buletin Hukum Perbankan dan Kebanksentralan Volume 4 Nomor 2 , 2006.

Hersinta, & Adithiyasanti.S. (2020). Social media, Youth and Environmental Low-risk Activism: a Case Study of Savesharks Indonesia Campaign on Twitter. ASPIRATION Journal, 2020: 113-134.

Hidayat, D. N. (2003) Paradigma dan Metodologi Penelitian Sosial Empirik Klasik. Jakarta: Departemen Ilmu Komunikasi FISIP Universitas Indonesia, 2003.

IMDb. Unfriended: Dark Web. March (2018). https://www.imdb.com/title/tt4761916/?ref_=fn_al_tt_4 (accessed Desember 20, 2020).

Manizar, E. (2016). Mengelola Kecerdasan Emosi. Tadrib Vol. IINo. 2, 2016: 1-16.

Mudjiono, Y. (2011). Kajian Semiotika dalam Film. Jurnal Ilmu Komunikasi, Vol. 1, No.1, 2011: 125-138.

Patton, M. Q. (2002). Qualitative Research and Evaluation Methods 3rdEdition. California: Thousand Oaks. Sage Publications Inc.

Piliang, Y. A. (2005). Cyberspace dan Perubahan Sosial: Eksistensi, Identitas, dan Makna. Jurnal Balairung Edisi 38/XIX, 2005.

Sarinastiti, N, & Vardhani. (2018). Internet dan Terorisme: Menguatnya Global Cyber-Terrorism Melalui New Media. Universitas Gadjah Mada, Vol 1, No. 1, 2018.

Sobur, A. (2012). Analisis Teks Media: Suatu Pengantar untuk Analisis Wacana, Analisis Semiotik dan Analisis Framing, Cetakan Keenam. Bandung: PT. Remaja Rosdakarya.

Supanto. (2016). Perkembangan Kejahatan Teknologi Informasi (cyber crime) dan Antisipasinya dengan Penal Policy. Yustisia. Vol.5 No.1, 2016: 52-70.

Utomo, K.D, J. Jupriono, & Beta, P.A. (2018). Film Dokumenter Gerakan Merekam Kotakarya Gresik Movie: Telaah Semiotika John Fiske. Jurnal Universitas 17 Agustus 1945 Surabaya.

Zuraida, M. (2015). Credit Card Fraud (Carding) dan Dampaknya Terhadap Perdagangan Luar Negeri Indonesia. Fakultas Ilmu Sosial dan Ilmu Politik Universitas Airlangga, Vol 4, No.1,

Scanned with CamScanner