Praxis: Jurnal Filsafat Terapan (2022) 1:1, 59-78
ISSN 1111-1111 | DOI: 10.11111/moderasi.xxxxxxx
Diterbitkan oleh FORIKAMI (Forum Riset Ilmiah Kajian Masyarakat Indonesia)
Tersedia online Pada Bulan Desember 2022.

Tindakan Hacking dan Profesi Hacker: Persoalan Etis antara Utilitarianisme dan Deontologi.

Richwen Canady, Mandalan, Desfantio Wuidjaja, Pradita University,
richwen.canady@student.pradita.ac.id

ABSTRACT: This research was conducted to see concrete evidence of the ethical theory of utilitarianism and the ethical theory of obligation or deontology on the issue of hackers as a profession and the act of hacking, where both of these things are still difficult to determine as a good thing or a bad thing because of the many types of hackers who have their own backgrounds and motives such as gray hat hackers and vigilante hackers. This research method is quantitative descriptive research, with data sources obtained from a survey method in the form of a questionnaire. The population in this study are people who know or have heard the concept of hackers and hacking, with a sample obtained through random sampling techniques totaling 100 respondents. The results of the questionnaire showed a division of respondents' opinions on several questions concerning the issue of gray hat hackers and vigilante hackers. Respondents' opinions on the concept of gray hat hackers and vigilante hacker were divided between agreed, strongly agreed, disagreed, and strongly disagreed. Agreeing and strongly agreeing opinions are a form of utilitarianism that recognizes gray hat hackers and vigilante hackers are a good thing because they are beneficial to most people, while disagreeing and strongly disagreeing opinions show a deontological view that considers gray hat hackers and vigilante hackers as a bad thing because hacking is an illegal act. By introducing the concepts of gray hat hackers and vigilante hackers, this research has successfully shown concrete evidence of both theories.

KEYWORDS: Hacking, Utilitarianism, Deontology, Gray Hat Hacker, Vigilante Hacker.

ABSTRAK: Penelitian ini dilakukan untuk melihat bukti nyata teori etika kemanfaatan atau utilitarianisme dan teori etika kewajiban atau deontologi pada persoalan *hacker* sebagai profesi dan tindakan *hacking,* di mana kedua hal tersebut masih sulit ditentukan sebagai suatu hal yang baik atau hal yang buruk karena banyaknya jenis hacker yang memiliki latar belakang dan motif masing-masing seperti *gray hat hacker* dan *vigilante hacker*. Metode penelitian ini adalah penelitian deskriptif kuantitatif, dengan sumber data yang diperoleh dari metode survei berbentuk kuesioner. Populasi pada penelitian ini merupakan orang yang mengetahui atau pernah mendengar konsep *hacker* dan *hacking*, dengan sampel yang diperoleh melalui teknik *random sampling* berjumlah 100 responden. Hasil kuesioner menunjukkan terbaginya pendapat responden terhadap beberapa pertanyaan yang menyangkut persoalan *gray hat hacker* dan *vigilante hacker*. Pendapat responden pada konsep *gray hat hacker* dan *vigilante hacker* terbagi menjadi setuju, sangat setuju, tidak setuju, dan sangat tidak setuju. Pendapat setuju dan sangat setuju adalah bentuk utilitarianisme yang mengakui *gray hat hacker* dan *vigilante hacker* adalah hal yang baik karena bermanfaat bagi kebanyakan orang, sedangkan tidak setuju serta sangat tidak setuju menunjukkan pandangan deontologi yang menilai *gray hat hacker* dan *vigilante*

hacker sebagai hal yang buruk karena peretasan atau *hacking* merupakan sebuah tindakan ilegal. Dengan mengenalkan konsep *gray hat hacker* dan *vigilante hacker*, penelitian ini telah berhasil memperlihatkan bukti nyata teori utilitarianisme dan teori deontologi.

KATA KUNCI: Hacking, Utilitarianisme, Deontologi, Gray Hat Hacker, Vigilante Hacker.

I. PENDAHULUAN

Kemajuan teknologi dan sistem informasi telah menghasilkan berbagai manfaat untuk umat manusia. Munculnya teknologi sistem informasi seperti internet telah memudahkan individu dalam pencarian informasi dan komunikasi. Tak hanya individu, perusahaan dan berbagai lembaga sudah mengimplementasikan teknologi sistem informasi untuk memudahkan proses manajemennya, penyimpanan data hingga bisnis mereka sendiri. Namun kemajuan ini secara tidak sengaja menimbulkan suatu ketergantungan.

Ketergantungan yang berasal dari kemudahan ini adalah bukti perubahan perilaku dan pola hidup manusia, dimana manusia sekarang menginginkan segala sesuatu menjadi serba cepat dan melupakan faktor keamanan (Utomo, 2019). Tanpa disadari, ketergantungan tersebut telah menimbulkan suatu permasalahan baru, yaitu munculnya jenis kejahatan baru c*yber crime* atau kejahatan siber. Salah satu contoh dari kejahatan siber yang sering didengar sekarang adalah tindakan peretasan atau *hacking*.

Perlu diketahui, istilah *hacking* sudah menjadi sangatlah kabur dikarenakan definisinya yang sudah mengalami perubahan. Awalnya, istilah "*hack*" mengacu pada cara inovatif untuk mencari solusi (Levy, 1984, dikutip dalam Tanczer, 2020). Namun *hacking* kemudian mendapat konotasi negatif yang merujuk pada tindakan peretasan, pencurian, dan perusakan. Hingga sekarang banyak penelitian yang sulit mendefinisikan apa itu *hacking* (Oliver, 2020).

Para pelaku yang melakukan tindakan *hacking* disebut dengan *hacker*. Menurut Oliver (2020), seorang *hacker* di jaman sekarang dapat didefinisikan sebagai pengguna yang ingin mendapatkan akses ke suatu target (seperti sistem, jaringan, grup, lembaga, atau perusahaan) dengan motif 1) mempelajari tentang target secara lebih lanjut, 2) mengeksploitasi target untuk diserang, atau 3) untuk menguntungkan masyarakat.

Negara Indonesia yang merupakan salah satu negara yang memiliki tingkat kepadatan penduduk yang tinggi di dunia, telah

mengalami dampak kejahatan siber *hacking*. *Hacking* yang termasuk dalam kejahatan siber di Indonesia pada tahun 2011 meningkat sebanyak 1,7% dibandingkan tahun lalu, di mana Indonesia menempati peringkat ke-28 (Arifah, 2011). Salah satu contoh kasus kejahatan siber *hacking* adalah kasus seorang *hacker* dengan sebutan Bjorka yang berhasil mendapatkan 44 juta data dari aplikasi MyPertamina dan kemudian dijual seharga 390 juta rupiah (Karina, 2022). Karena *hacking* kejahatan siber ini, banyak orang yang menilai hacking akan selalu menimbulkan dampak negatif.

Namun sebenarnya, *hacking* jika dilakukan secara etis bisa bermanfaat bagi suatu perusahaan. Seorang hacker dengan nilai etika tinggi dapat membantu perancangan sistem dengan mencari celah pada sistem tersebut, sehingga kualitas keamanan sistem tersebut bisa ditingkatkan lagi (Utomo, 2019).

Oleh karena itu, tindakan *hacking* dan para *hackers* masih belum bisa disimpulkan secara jelas apakah baik atau buruk dari sudut pandang etika. Maka banyak peneliti yang berusaha untuk mengkategorikan hacker, sehingga muncul konsep *Hacker's Hat*. Menurut Utomo (2019), *Hacker* memiliki tiga kategori yang berbeda yaitu *White Hat Hacker, Black Hat Hacker, dan Grey Hat Hacker.*

White Hat Hacker merupakan seorang hacker yang berfokus pada cara kerja keamanan sistem komputer. *White Hat Hacker* bertujuan untuk mencari kelemahan dalam sistem, tidak bertujuan untuk merusak keamanan sistem, kemudian *White Hat Hacker* melakukan tindakan tersebut sebagai menguji penetrasi atau pentesting untuk memberikan solusi kepada pemilik sistem. Konsep *White Hat Hacker* atau *Ethical Hacker* sudah banyak diimplementasikan di berbagai perusahaan di dunia, di mana profesi tersebut disewa untuk mengetes keamanan sistem perusahaan. Sedangkan *Black Hat Hacker* adalah peretas yang paling berbahaya karena tujuan mereka adalah mengambil keuntungan untuk diri mereka sendiri, mereka adalah peretas yang secara ilegal dapat memasuki sistem dan mencuri informasi sensitif dan kemudian menjualnya untuk mendapatkan uang atau merusak sistem (Utomo, 2019).

Gray Hat Hacker adalah campuran dari *White Hat Hacker* dan *Black Hat Hacker*. Peretas yang sulit dikatakan baik atau buruk, terkadang mereka menyerang tanpa izin hanya untuk bersenang-senang, atau terkadang bisa menjadi penasihat keamanan untuk melindungi sistem dengan syarat membutuhkan biaya (Utomo, 2019).

Ketiga kategori tersebut merupakan 3 jenis utama seorang *hacker*, namun masih banyak jenis hacker lainnya yang memiliki latar belakang, tujuan, dan cara masing-masing. Contohnya adalah konsep *vigilante hacker*.

Vigilantisme berasal dari bahasa Spanyol yang berarti penjaga, kata ini dapat ditelusuri kembali ke kata latin "*vigilare*" yang berarti terus sadar atau bangun. Ketika seseorang main hakim sendiri, mereka disebut melakukan aktifitas *vigilante* (Whitton, 2007). Menurut Tiller (2004), vigilantisme merupakan salah satu dari ke 4 aspek yang dapat membedakan klasifikasi *hacker*. *Vigilante hacker* menyerang sistem dengan tujuan untuk menghakimi tindakan buruk yang dilakukan seseorang atau grup. Hal ini tentunya semakin mengundang berbagai pertanyaan etika, hukum, dan moralitas terkait tindakan *hacking*.

Terdapat beberapa teori etis bagaimana cara seseorang bisa memandang tindakan *hacking* ini, seperti 2 teori yang saling bertolak belakang yaitu etika kemanfaatan (utilitarianisme) dan etika kewajiban (deontologi).

Utilitarianisme berasal dari kata Latin "*utilis*", yang berkembang menjadi kata bahasa Inggris *"utility*", yang memiliki arti manfaat (Bertens, 2000 dikutip dalam Kumalasari, 2021). Teori ini menyatakan suatu tindakan bisa dikatakan baik jika menghasilkan manfaat bagi kebanyakan orang, atau dalam istilah yang terkenal "kebahagiaan terbesar untuk jumlah terbesar" (Kumalasari, 2021). Deontologi berasal dari kata Yunani "*deont*" yang berarti kewajiban atau mengikat, merupakan pandangan Immanuel Kant (1724-1804) yang menilai suatu tindakan berdasarkan kebenaran secara moral kebanyakan orang, tanpa melihat konsekuensinya (Barrow, 2022). Deontologi mengutamakan tindakan atas konsekuensi, sedangkan utilitarianisme mementingkan konsekuensi atau hasil dibanding tindakan (Gray & Schein, 2012).

Kedua teori tersebut merupakan contoh cara pandang seseorang terhadap persoalan *hacking* dan *hacker*, yang di mana selama dampak tindakan peretasan ilegal tersebut menguntungkan masyarakat banyak, maka tindakan tersebut bisa tergolong baik dan benar jika mengikuti teori utilitarianisme. Sedangkan deontologi akan memandang persoalan ini secara negatif dan dianggap melanggar moral. Karena *hacking* pada dasarnya adalah upaya tindakan membobol sesuatu yang dilindungi, dan dampak positif yang diperoleh tidak bisa membenarkan upaya tersebut.

Berdasarkan latar belakang serta definisi-definisi tersebut, peneliti mencoba melakukan penelitian terhadap cara pandang orang terhadap *hacking* dan *hacker* jika mereka diberi tahu konsep *gray hat hacker* dan *vigilante hacker*, agar bisa dilihat bentuk nyata dari etika kemanfaatan dan etika kewajiban.

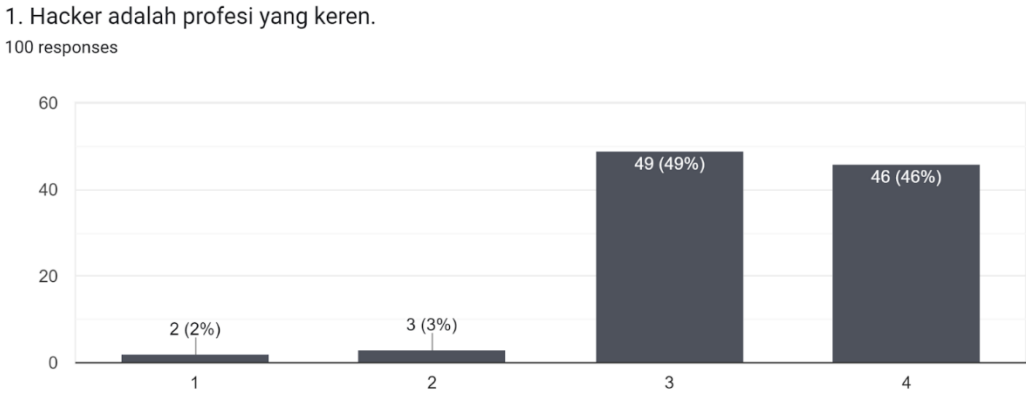
II. METODE

Penelitian "Profesi Hacker dan Tindakan Hacking: Persoalan Etis antara Etika Kemanfaatan dan Kewajiban" merupakan penelitian deskriptif, yaitu penelitian yang memaparkan informasi, fakta, gejala, serta kejadian secara akurat, untuk mengetahui sifat suatu populasi, tanpa perlu dihubungkan atau diuji hipotesis (Hardani dkk, 2020). Sumber data diperoleh menggunakan metode survei dengan instrumen kuesioner. Populasi pada penelitian yang dilakukan adalah orang yang pernah mendengar *hacking* dan *hacker* dimana sampel diperoleh menggunakan teknik *random* sampling dengan jumlah 100 responden. Nilai skor yang digunakan adalah berdasarkan Skala Likert di mana pengkategorian nilai menggunakan empat kategori yakni, sangat tidak setuju, tidak setuju, setuju, dan sangat setuju

Tabel 1. Keterangan Kategori Skor

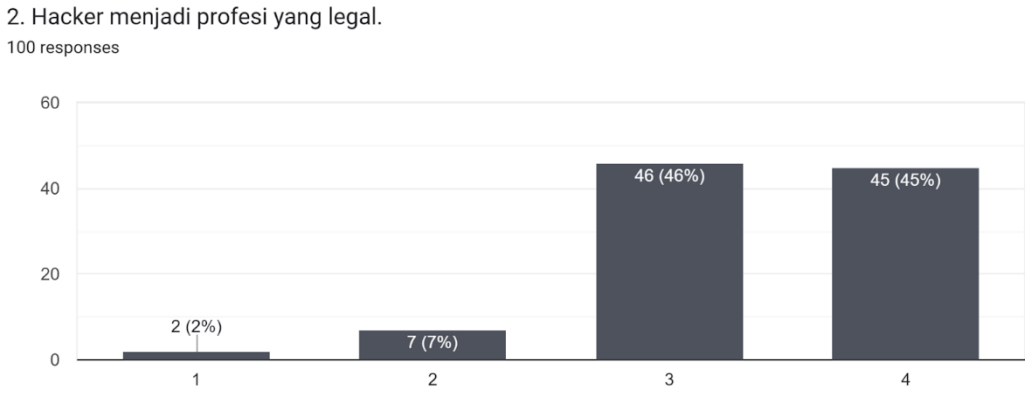
Skor	Keterangan	Simbol
1	Sangat Tidak Setuju	**STS**
2	Tidak Setuju	**TS**
3	Setuju	**S**
4	Sangat Setuju	**SS**

III. HASIL



Gambar 1. Grafik Kekaguman Responden Terhadap *Hacker*.

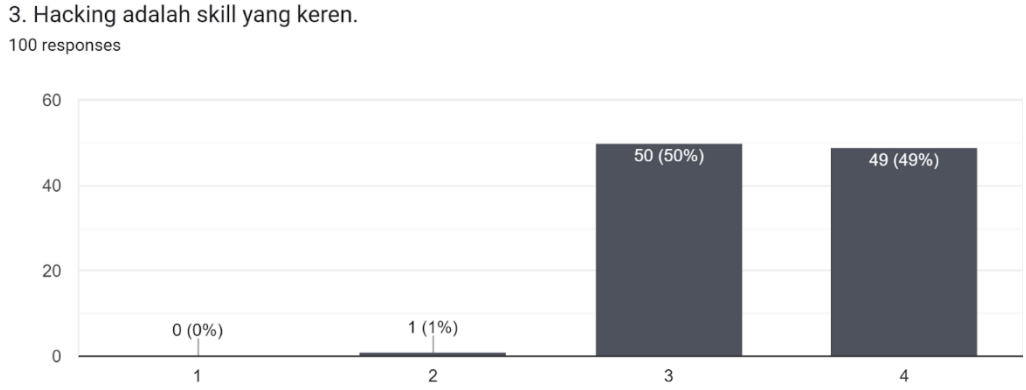
Berdasarkan gambar 1, diketahui pendapat responden terhadap pernyataan "*Hacker* adalah profesi yang keren" adalah responden menyatakan sangat tidak setuju ada 2 orang atau sebesar (2%), terdapat 3 orang menyatakan tidak setuju atau sebesar (3%), terdapat 49 orang menyatakan setuju atau sebesar (49%), terdapat 46 orang menyatakan sangat setuju atau sebesar (46%). Berdasarkan hasil data yang telah diperoleh dapat disimpulkan bahwa responden mengagumi para *hacker*.



Gambar 2. Grafik Pendapat Responden terhadap *Hacker* menjadi Profesi Legal.

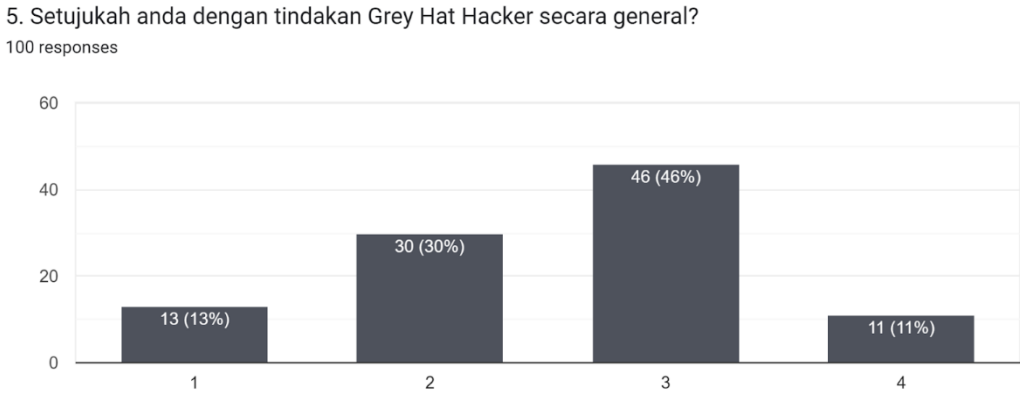
Berdasarkan gambar 2, diketahui pendapat responden terhadap pernyataan "*Hacker* menjadi profesi yang legal" adalah responden

menyatakan sangat tidak setuju ada 2 orang atau sebesar (2%), terdapat 7 orang menyatakan tidak setuju atau sebesar (7%), terdapat 46 orang menyatakan (46%), terdapat 45 orang menyatakan sangat setuju atau sebesar (45%). Berdasarkan hasil data yang telah diperoleh dapat disimpulkan bahwa mayoritas responden menginginkan *hacker* menjadi profesi yang legal.



Gambar 3. Grafik Kekaguman Responden terhadap Kemampuan *Hacking*.

Berdasarkan gambar 3, diketahui pendapat responden terhadap pernyataan "*Hacking* adalah *skill* yang keren" adalah 0 responden menyatakan sangat tidak setuju dengan pernyataan hacking adalah skill yang keren, terdapat 1 orang menyatakan tidak setuju atau sebesar (1%), terdapat 50 orang menyatakan setuju atau sebesar (50%), terdapat 49 orang menyatakan sangat setuju atau sebesar (49%). Berdasarkan hasil data yang telah diperoleh dapat disimpulkan bahwa mayoritas responden mengagumi kemampuan *hacking*.



Gambar 4. Pendapat Responden untuk *Gray Hat Hacker*.

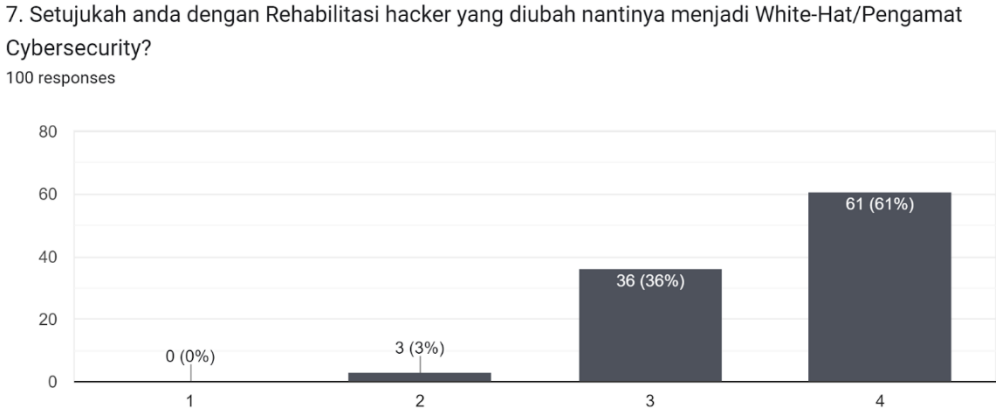
Berdasarkan gambar 4, diketahui pendapat responden terhadap pertanyaan "Setujukah anda dengan tindakan Grey Hat Hacker secara general/umum?" adalah 13 orang menyatakan sangat tidak setuju atau sebesar (13%), terdapat 30 orang menyatakan tidak setuju atau sebesar (30%), terdapat 48 orang menyatakan setuju atau sebesar (40%), terdapat 11 orang menyatakan setuju atau sebesar (11%).

Gambar 5. Grafik Pendapat Responden terhadap *Gray Hat Hacker* dengan Skenario.

Responden diberikan skenario di mana ada suatu perusahaan yang tidak mempedulikan keamanan data yang menyangkut data pribadi konsumer perusahaan tersebut. Responden kemudian ditanya setuju atau tidaknya mereka apabila seorang *gray hat hacker* menyerang

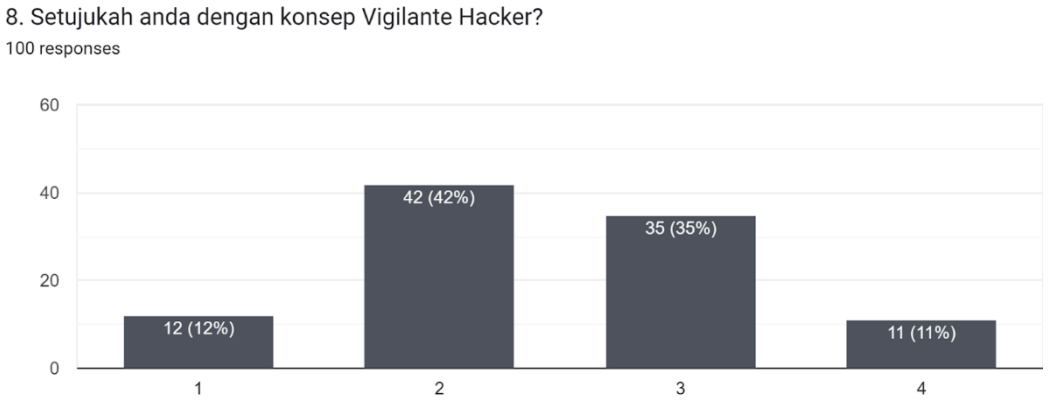
perusahaan tersebut untuk memperingati perusahaannya tanpa meminta ijin terlebih dahulu.

Berdasarkan gambar 5 diketahui pendapat responden terhadap skenario tersebut adalah 4 orang menyatakan sangat tidak setuju atau sebesar (4%), terdapat 21 orang menyatakan tidak setuju atau sebesar (21%), terdapat 43 orang menyatakan setuju atau sebesar (43%), terdapat 32 orang menyatakan sangat setuju atau sebesar (32%). Berdasarkan hasil data yang diperoleh dapat disimpulkan bahwa mayoritas responden setuju dengan perbuatan *gray hat hacker* pada skenario tersebut.



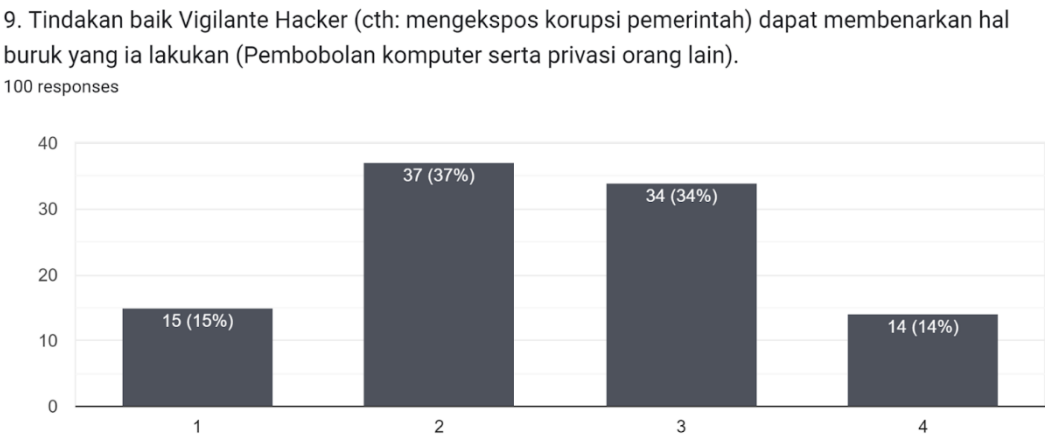
Gambar 6. Grafik Pendapat Responden terhadap Rehabilitasi *Hacker*.

Berdasarkan gambar 6 diketahui pendapat responden terhadap pertanyaan "Setujukah anda dengan Rehabilitas hacker yang diubah nantinya menjadi *White-Hat*/Pengamat *Cybersecurity*?" adalah 0 orang menyatakan sangat tidak setuju, terdapat 3 orang menyatakan tidak setuju atau sebesar (3%), terdapat 30 orang menyatakan setuju atau sebesar (30%), terdapat 61 orang menyatakan sangat setuju atau sebesar (61%). Berdasarkan hasil data yang diperoleh dapat disimpulkan bahwa mayoritas responden setuju dengan rehabilitas untuk para *hacker* yang tertangkap.



Gambar 7. Grafik Pendapat Responden terhadap *Vigilante Hacker.*

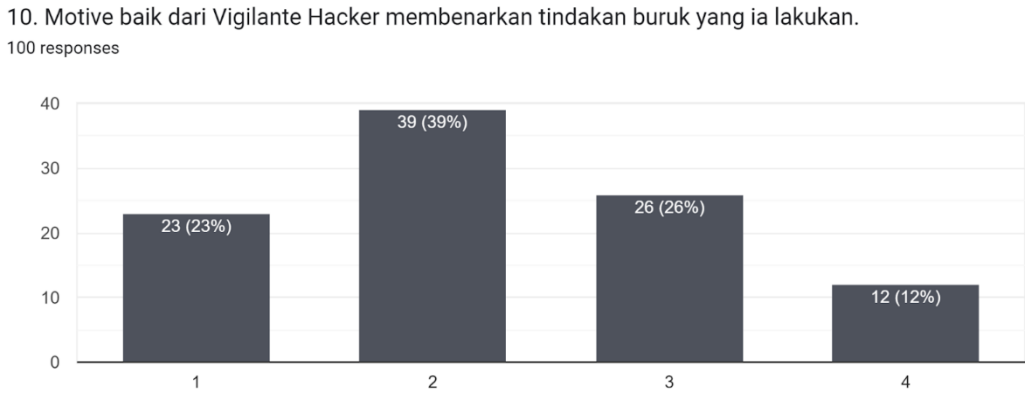
Berdasarkan gambar 7 diketahui pendapat responden terhadap pertanyaan "Setujukah anda dengan konsep *Vigilante Hacker*?" adalah 12 orang menyatakan sangat tidak setuju atau sebesar (12%), terdapat 42 orang menyatakan tidak setuju atau sebesar (42%), terdapat 36 orang menyatakan setuju atau sebesar (36%), terdapat 11 orang menyatakan sangat setuju atau sebesar (11%).



Gambar 8. Grafik Pendapat Responden terhadap Tindakan *Vigilante Hacker.*

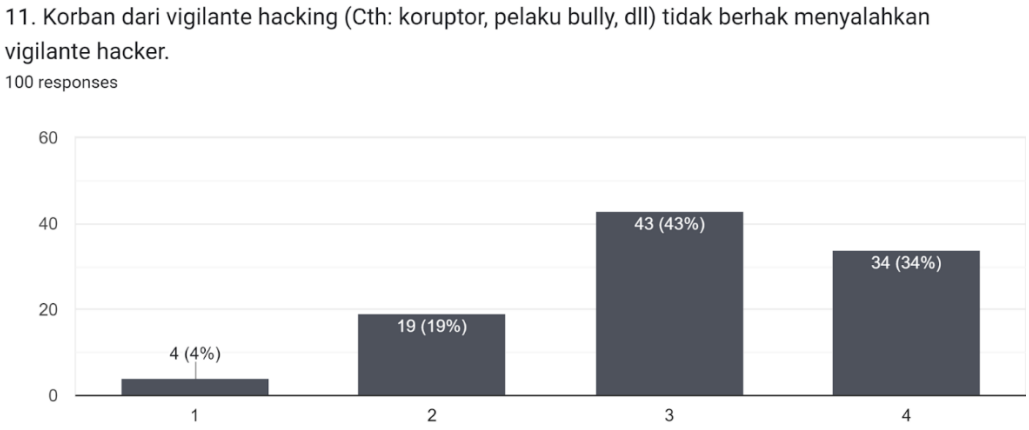
Berdasarkan gambar 8 diketahui pendapat responden terhadap pernyataan "Tindakan baik *Vigilante Hacker* dapat membenarkan hal buruk yang ia lakukan" adalah 15 orang menyatakan sangat tidak setuju

atau sebesar (15%), terdapat 37 orang menyatakan tidak setuju atau sebesar (37%), terdapat 34 orang menyatakan setuju atau sebesar (34%), terdapat 14 orang menyatakan sangat setuju (14%).



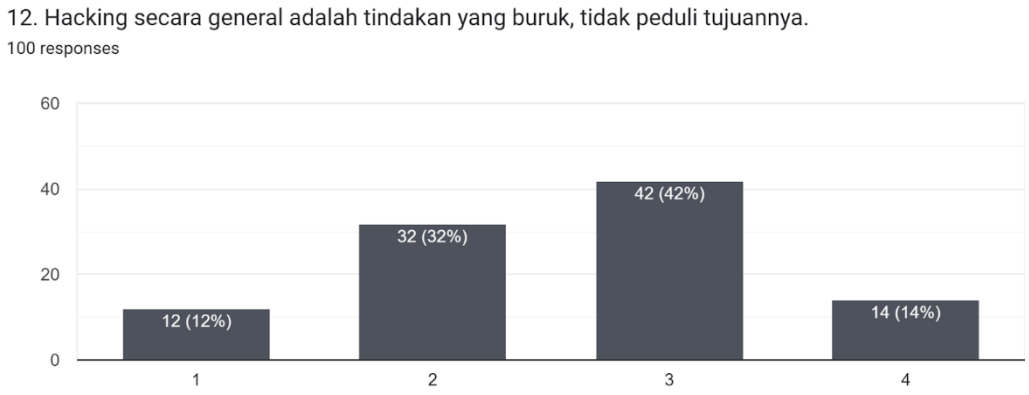
Gambar 9. Grafik Pendapat Responden terhadap Niat/Motif *Vigilante Hacker*.

Berdasarkan gambar 9 diketahui pendapat responden terhadap pernyataan "Motive baik dari *Vigilante Hacker* membenarkan tindakan buruk yang ia lakukan." adalah 23 orang menyatakan sangat tidak setuju atau sebesar (23%), terdapat 39 orang menyatakan tidak setuju atau sebesar (39%), terdapat 26 orang menyatakan setuju atau sebesar (26%), terdapat 12 orang menyatakan sangat setuju atau sebesar (12%).



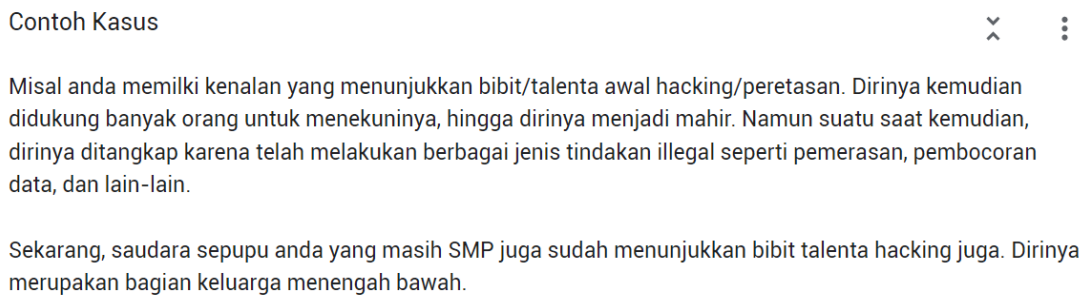
Gambar 10. Grafik Pendapat Responden terhadap Korban dari *Vigilante Hacking*.

Berdasarkan gambar 10 diketahui pendapat responden terhadap pernyataan "Korban dari *vigilante hacking* (cth: koruptor, pelaku perundungan, dll) tidak berhak menyalahkan *vigilante hacker*" adalah 4 orang menyatakan sangat tidak setuju atau sebesar (4%), 19 orang menyatakan (19%), terdapat 43 orang menyatakan setuju atau sebesar (43%), terdapat 34 orang menyatakan sangat setuju atau sebesar (34%). Berdasarkan hasil data yang diperoleh dapat disimpulkan bahwa mayoritas responden setuju terhadap pendapat bahwa korban yang telah diekspos *vigilante hacking* tidak berhak menyalahkan *vigilante hacker*.



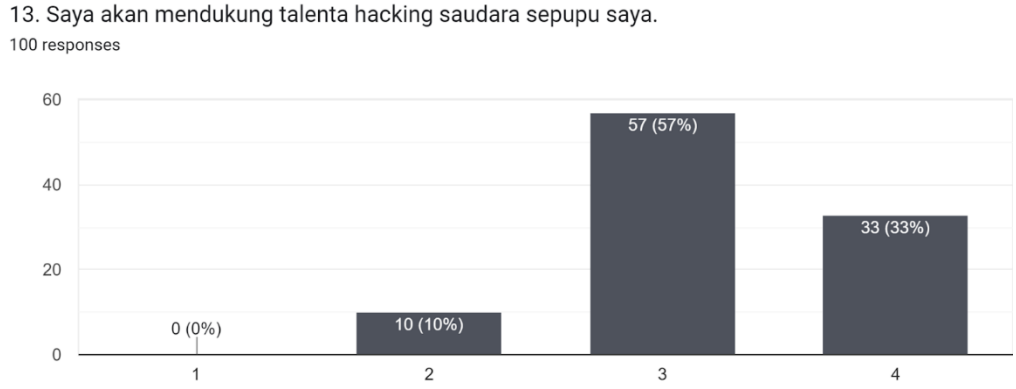
Gambar 11. Grafik Pendapat Responden terhadap *Hacking*.

Berdasarkan gambar 11 diketahui pendapat responden terhadap pernyataan "*Hacking* secara general adalah tindakan yang buruk, tidak peduli tujuannya." adalah 12 orang menyatakan sangat tidak setuju atau sebesar (12%), terdapat 32 orang menyatakan tidak setuju atau sebesar (32%), terdapat 43 orang menyatakan setuju atau sebesar (42%), terdapat 14 orang menyatakan sangat setuju atau sebesar (14%).



Gambar 12. Contoh Skenario Kekerabatan.

Seperti pada gambar 12, responden telah diberikan skenario di mana mereka memiliki kenalan bertalenta *hacking* yang didukung banyak orang, namun kenalannya ditangkap oleh pihak berwenang karena telah menyalahgunakan talenta tersebut. Beberapa pertanyaan selanjutnya adalah mengenai pendapat responden apabila ternyata kerabat responden juga memiliki talenta *hacking*. Skenario ini dibuat untuk mengetahui apakah akan ada perubahan pendapat jika keluarga dan teman disangkutpautkan.

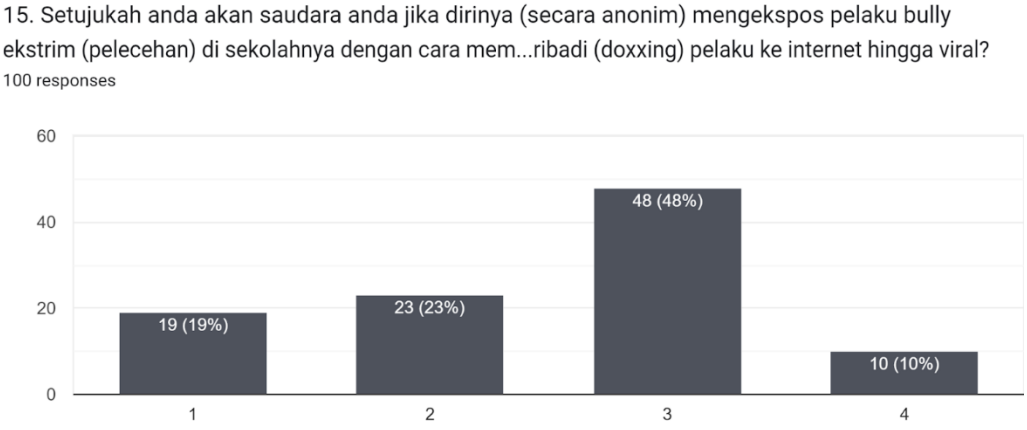


Gambar 13. Grafik Pendapat Responden terhadap Talenta *Hacking*.

Berdasarkan gambar 13 diketahui pendapat responden terhadap pernyataan "Saya akan mendukung talenta *hacking* saudara sepupu saya." pada skenario gambar 13 adalah 0 orang menyatakan sangat tidak setuju atau sebesar (0%), terdapat 10 orang menyatakan tidak setuju atau sebesar (10%), terdapat 57 orang menyatakan setuju atau sebesar (57%), terdapat 33 orang menyatakan sangat setuju atau sebesar (33%). Berdasarkan hasil data yang diperoleh dapat disimpulkan bahwa mayoritas responden setuju untuk tetap mendukung talenta kerabatnya.

Gambar 14. Grafik Pendapat Responden terhadap *Gray Hat Hacker* setelah Skenario.

Berdasarkan gambar 14 diketahui pendapat responden terhadap pernyataan "Setujukah anda akan saudara anda jika dirinya berniat menjadi *Grey Hat Hacker* untuk mendapatkan uang di usia mudanya?" pada skenario gambar 14 adalah 24 orang menyatakan sangat tidak setuju atau sebesar (24%), terdapat 36 orang yang menyatakan tidak setuju atau sebesar (36%), terdapat 32 orang menyatakan setuju atau sebesar (32%), terdapat 8 orang menyatakan sangat setuju atau sebesar (8%).



Gambar 15. Grafik Pendapat Responden terhadap *Gray Hat Hacker* setelah Skenario.

Responden diberikan skenario lanjutan dimana kerabat responden (secara anonim) diberikan kesempatan untuk mengekspos informasi pelaku perundungan ekstrim di sekolahnya ke internet setelah membobol akun pelaku. Berdasarkan gambar 15 diketahui tanggapan responden terhadap skenario lanjutan tersebut adalah 19 orang menyatakan sangat tidak setuju atau sebesar (19%), terdapat 23 orang menyatakan tidak setuju atau sebesar (23%), terdapat 48 orang menyatakan setuju atau sebesar (48%), terdapat 10 orang menyatakan sangat setuju atau sebesar (10%).

IV. PEMBAHASAN

Penelitian ini membahas tentang bentuk nyata terbaginya cara pandang orang terhadap hacking dan hacker menjadi 2 yaitu cara pandang etika kemanfaatan dan etika kewajiban. Cara pandang yang dimaksud dalam penelitian ini berdasarkan teori yang sebelumnya disampaikan di pendahuluan, teori utilitarianisme dan deontologi. Teori utilitarianisme menyatakan suatu tindakan bisa dikatakan baik jika menghasilkan manfaat bagi kebanyakan orang, atau dalam istilah yang terkenal "kebahagiaan terbesar untuk jumlah terbesar" (Kumalasari, 2021). Teori deontologi menilai suatu tindakan berdasarkan kebenaran secara moral kebanyakan orang, tanpa melihat konsekuensinya (Barrow, 2022).

Gray Hat Hacker adalah campuran dari *White Hat Hacker* dan *Black Hat Hacker*. Peretas yang sulit dikatakan baik atau buruk, terkadang mereka menyerang tanpa ijin hanya untuk bersenang-senang, atau terkadang bisa menjadi penasihat keamanan untuk melindungi sistem dengan syarat membutuhkan biaya (Utomo, 2019). Pada pertanyaan kuesioner terkait dengan pendapat responden terhadap *gray hat hacker*, berdasarkan gambar 4, hasil respon terbagi menjadi 46 setuju (46%) 11 sangat setuju (11%) melawan 30 tidak setuju (30%) 13 sangat tidak setuju (13%). Pendapat setuju merupakan bentuk pandangan utilitarianisme yang dimana responden menilai tindakan *gray hat hacker* bermanfaat, sedangkan tidak setuju adalah bentuk pandangan deontologi dimana mereka menilai tindakan *gray hat hacker* buruk karena mereka belum meminta izin. Pendapat responden terbagi, namun sedikit condong ke

arah setuju yang dimana adalah bentuk utilitarianisme. Responden diasumsikan merasa dampak positif *gray hat hacking* berguna untuk banyak orang sehingga responden sedikit menoleransi tindakan tersebut.

Vigilante hacker adalah hacker yang menyerang sistem dengan tujuan untuk menghakimi tindakan buruk yang dilakukan seseorang atau grup (Tiller, 2004). Pada pertanyaan kuesioner terkait dengan pendapat responden terkait *vigilante hacker*, berdasarkan gambar 7, hasil respon terbagi menjadi 35 setuju (35%) 11 sangat setuju (11%) melawan 42 tidak setuju (42%) 12 sangat tidak setuju (12%). Pada gambar 8, hasil respon terbagi menjadi 34 setuju (34%) 14 sangat setuju (14%) melawan 37 tidak setuju (37%) 15 sangat tidak setuju (15%). Pendapat setuju merupakan bentuk pandangan utilitarianisme yang dimana responden menilai tindakan *vigilante hacker* bermanfaat untuk banyak orang sehingga membenarkan tindakan pembobolan yang ia lakukan, sedangkan tidak setuju adalah bentuk pandangan deontologi dimana responden menilai tindakan *vigilante hacker* sebagai buruk karena mereka beraksi diatas hukum dan melakukan tindakan ilegal. Hasil respon sekali lagi menunjukkan pendapat responden terbagi ditengah-tengah, namun pada persoalan ini pendapat responden sedikit condong ke arah tidak setuju atau deontologi. Responden diasumsikan sedikit tertarik dengan dampak positifnya, namun tetap merasa bahwa *vigilante hacker* sebagai konsep yang salah karena perbuatan ilegalnya.

Penelitian ini juga menemukan informasi lain yaitu pada skenario hipotetis dimana jika saudara responden juga menunjukkan bakat kemampuan hacking. Skenario tersebut dibuat untuk mengetahui apakah faktor kekerabatan akan mempengaruhi cara pandang seseorang terhadap hacking. Pada gambar 13, respon didominasi oleh setuju (57%) dan sangat setuju (33%). Jumlah hasil tidak terlalu berbeda dengan pendapat awal responden terhadap hacking dan hacker secara umum seperti pada gambar 1 dan gambar 2. Responden tetap memilih untuk mendukung talenta kerabat mereka. Pada gambar 14 ditemukan sedikit perubahan pendapat responden terhadap *gray hat hacker*, pada gambar 14 responden tetap terbagi secara utilitarianisme dan deontologi, namun jumlah tidak setuju (36%) dan sangat tidak setuju (24%) menjadi sedikit

lebih banyak dibanding setuju (32%) dan sangat setuju (8%). Hal ini menunjukkan faktor kekerabatan akan sedikit berpengaruh dengan cara pandang etika seseorang terhadap suatu situasi. Asumsi kesimpulan penelitian ini adalah responden tidak ingin kerabat atau saudara sepupu mereka sendiri menjadi seorang *gray hat hacker*.

VI. CONCLUSION

Penelitian ini telah membahas persepsi dan cara pandang responden terhadap persoalan-persoalan etis yang ada pada pernyataan kuesioner. Dengan mengenalkan konsep gray hat hacker dan vigilante hacker kepada responden, penelitian ini berhasil memperlihatkan bentuk nyata kedua teori pandangan etika yaitu etika kemanfaatan (utilitarianisme) dan etika kewajiban (deontologi). Berdasarkan hasil kuesioner tersebut, didapatkan kesimpulan bahwa kedua teori utilitarianisme dan deontologi berlaku juga terhadap persoalan hacking dan hacker. Hal ini dibuktikan dengan jumlah setuju dan tidak setuju pada beberapa pertanyaan kuesioner yang tidak berbeda jauh. Pendapat masing-masing responden telah terbagi dan menunjukkan sifat yang sesuai dengan kedua teori. Di sisi lain, penelitian ini juga menemukan beberapa kasus tertentu dimana hampir seluruh responden memiliki satu pendapat yang sama, seperti kekaguman responden terhadap kemampuan hacking. Selain itu, hampir seluruh responden juga memiliki keinginan untuk tetap mendukung kerabat yang memiliki talenta hacking meskipun pendapat mereka sebelumnya terbagi. Ditemukan juga faktor kekerabatan ternyata akan sedikit mempengaruhi pandangan responden terhadap gray hat hacker sebagai profesi, di mana responden diasumsikan tidak menginginkan kerabat mereka menjadi seorang gray hat hacker.

Dengan apa yang sudah disampaikan, penelitian ini tidak lepas dari kesalahan. Terbatasnya jumlah responden sampel yang bisa diperoleh membuat penelitian ini jauh dari kata sempurna, sehingga dibutuhkan penelitian lebih lanjut yang membutuhkan penambahan jumlah responden, serta pencarian faktor-faktor lain yang mungkin bisa mempengaruhi pandangan etika seseorang.

DAFTAR REFERENSI

Arifah, D. A. (2011). Kasus cybercrime di indonesia. jurnal Bisnis dan Ekonomi, 18(2). Retrieved from https://unisbank.ac.id/ojs/index.php/fe3/article/view/2099/767

Barrow, J. M., & Khandhar, P. B. (2022). Deontology. StatPearls Publishing, Treasure Island (FL). http://europepmc.org/books/NBK459296

Gray, K., & Schein, C. (2012). Two Minds Vs. Two Philosophies: Mind Perception Defines Morality and Dissolves the Debate Between Deontology and Utilitarianism. Review of Philosophy and Psychology, 3. https://doi.org/10.1007/s13164-012-0112-5

Hardani, H., Andriani, H., Fardani, R. A., Ustiawaty, J., Utami, E. F., Sukmana, D. J., & Istiqomah, R. R. (2020). Buku Metode penelitian kualitatif & kuantitatif. Yogyakarta: Pustaka Ilmu.

Karina, D. (2022, November 11). 44 Juta Data MyPertamina Diduga Bocor, Pertamina dan Telkom Bakal Investigasi. Kompas TV. Retrieved from https://www.kompas.tv/article/347339/44-juta-data-mypertamina-diduga-bocor-pertamina-dan-telkom-bakal-investigasi

Kumalasari, V. (2021). ETIKA PROFESI, Dalam Bidang Teknologi Informasi. Penerbit Yayasan Prima Agus Teknik, 1-75. Retrieved from https://digilib.stekom.ac.id/assets/dokumen/ebook/feb_b48db5b7d841a92b6dbd5a6209a3f41107806e45_1642141125.pdf.

Levy, S. (1984). Hackers: Heroes of the computer revolution (Vol. 14). Garden City, NY: Anchor Press/Doubleday.

Tanczer, L. M. (2020). 50 shades of hacking: How IT and cybersecurity industry actors perceive good, bad, and former hackers. Contemporary Security Policy, 41(1), 108–128. https://doi.org/10.1080/13523260.2019.1669336

Tiller, J. S. (2004). The ethical hack: a framework for business value penetration testing. Auerbach publications.

Utomo, G. A. (2019). Ethical hacking. Cyber Security dan Forensik Digital, 2(1), 8-15.

Vivi Kumalasari. (2021). ETIKA PROFESI, Dalam Bidang Teknologi Informasi. Penerbit Yayasan Prima Agus Teknik, 7(1), 1-75. Retrieved from https://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/249

Whitton, A. (2007). Vigilantism, Vigilante Justice, and Victim Self-Help.