

Digital Forensik *Deleted Cyber Crime Evidence* pada Pesan Instan Media Sosial

Digital Forensics Deleted Cyber Crime Evidence on Social Media Instant Messaging

Rahmat Novrianda Dasmen¹, Ferry Kurniawan²

¹Teknik Komputer, Universitas Bina Darma

²Sastra Inggris, Universitas Bina Darma

E-mail: ¹rahmat.novrianda.d@gmail.com, ²ferry.kurniawan@binadarma.ac.id

Abstrak

Cyber crime merupakan tindak kejahatan yang terjadi di dunia maya, yang mana salah satu *cyber crime* paling marak terjadi adalah *cyberbullying* pada remaja. Adapun dari hasil survei diperoleh bahwa terdapat 2 pesan instan dari media sosial yang paling sering digunakan, yaitu *Facebook Messenger* dan *Whatsapp*. Oleh sebab itu, *cyber crime* juga kemungkinan besar terjadi pada kedua pesan instan tersebut karena penggunaannya sangat dominan. Melihat perkembangan IoT yang mempengaruhi setiap kegiatan melalui komunikasi di dunia maya, maka bukti digital dari pesan instan di media sosial saat ini telah menjadi bukti yang valid dalam mengungkap berbagai persoalan, salah satunya *cyberbullying*. Akan tetapi, tindak kejahatan akan sulit diungkap jika bukti digital tersebut terhapus atau sengaja dihapus. Oleh karena itu, pada penelitian dengan Metode *Action Research* ini, penulis melakukan proses Digital Forensik untuk mengungkap bukti *cyberbullying* dari *Facebook Messenger* dan *Whatsapp*. Dalam hal ini, *cyberbullying* hanyalah contoh kecil dari sekian banyak *cyber crime* yang terjadi. Oleh karena itu, proses Digital Forensik ini dapat diterapkan untuk mengungkap berbagai jenis *cyber crime* lainnya. Selain itu, hasil dari penelitian ini juga dapat digunakan untuk mengungkap bukti-bukti digital lain yang dibutuhkan dalam proses penyidikan.

Kata kunci: *Cyber Crime*, *Cyber Bullying*, Digital Forensik, *Facebook Messenger*, *Whatsapp*.

Abstract

Cyber crime is a crime that occurs in cyberspace, where one of the most prevalent cyber crimes is cyberbullying in adolescents. The survey results show that there are 2 instant messages from the most frequently used social media, namely Facebook Messenger and Whatsapp. Therefore, cyber crime is also likely to occur in the two instant messages because the users are very dominant. Seeing the development of IoT that affects every activity through communication in cyberspace, digital evidence from instant messages on social media has now become valid evidence in uncovering various problems, one of which is cyberbullying. However, crimes will be difficult to uncover if the digital evidence is deleted or intentionally deleted. Therefore, in this study using the Action Research Method, the authors carried out a Digital Forensic process to uncover evidence of cyberbullying from Facebook Messenger and Whatsapp. In this case, cyberbullying is only a small example of the many cyber crimes that occur. Therefore, this Digital Forensics process can be applied to reveal various other types of cyber crimes. In addition, the results of this study can also be used to reveal other digital evidence needed in the investigation process.

Keywords: *Cyber Crime*, *Cyber Bullying*, Digital Forensic, *Facebook Messenger*, *Whatsapp*.

1. PENDAHULUAN

Cyber Crime ataupun kejahatan di dunia maya saat ini semakin marak terjadi melalui berbagai media komunikasi digital. Adapun dari hasil penelitian Kementerian Komunikasi dan Informatika dibantu oleh UNICEF yang dipublikasikan pada bulan Februari Tahun 2004, dimana dalam rentang tahun 2011 hingga 2013 diperoleh pernyataan bahwa hampir seluruh remaja di Negara Indonesia mengaku sebagai korban kejahatan dunia maya yaitu *cyberbullying*. Hasil penelitian ini diperoleh dari survei dengan 400 responden dengan rentang usia 10 hingga 19 Tahun, dimana 89% responden memanfaatkan media sosial untuk komunikasi dengan teman-temannya, 56% responden menggunakan media sosial untuk komunikasi dengan keluarga dan 35% responden melakukan komunikasi dengan gurunya menggunakan media sosial. Adapun dari hasil penelitian tersebut, ditemukan bahwa 13% responden mengakui bahwa mereka memperoleh hinaan serta ancaman yang merupakan bentuk *cyberbullying* [1]. Dapat diketahui bahwa *cyberbullying* yang merupakan salah satu *cyber crime* ini merupakan dampak negatif yang dirasakan dari berkembangnya media digital [2]. *Cyberbullying* ataupun tindak *bullying* di dunia maya, yang mana *bullying* merupakan suatu tindakan yang membuat korbannya trauma, merasa tertekan hingga tidak berdaya karena pelaku menyakiti korban dengan perkataan, fisik hingga serangan terhadap psikologi korban [3].

Cyber crime yang merupakan dampak negatif dari perkembangan *Internet of Thing*, yang mana IoT merupakan suatu konsep penggunaan *internet* untuk beberapa hal tanpa harus adanya pertemuan langsung antara manusia dengan manusia [4]. Oleh karena perkembangan IoT yang semakin pesat, maka semakin meningkat juga *cyber crime* sehingga saat ini bukti digital telah menjadi bukti (*evidence*) yang valid untuk dibawa ke meja persidangan. Akan tetapi, akan menjadi permasalahan yang rumit jika bukti digital tersebut terhapus atau sengaja dihapus. Oleh karena itu, penelitian ini bertujuan untuk mengungkapkan bukti-bukti digital yang sudah terhapus, yang mana memerlukan suatu Teknik untuk menarik bukti *cyber crime* yang telah terhapus (*Deleted Cyber Crime Evidence*) yaitu Teknik Digital Forensik. Adapun Digital Forensik adalah bidang ilmu forensik yang khusus melakukan penyelidikan terhadap bukti *cyber crime* dari perangkat digital ataupun media digital yang digunakan [5]. Dari hasil penelitian sebelumnya, diperoleh bahwa Teknik Digital Forensik semakin sering digunakan dalam penanganan pengungkapan bukti digital dari *cyber crime* [6].

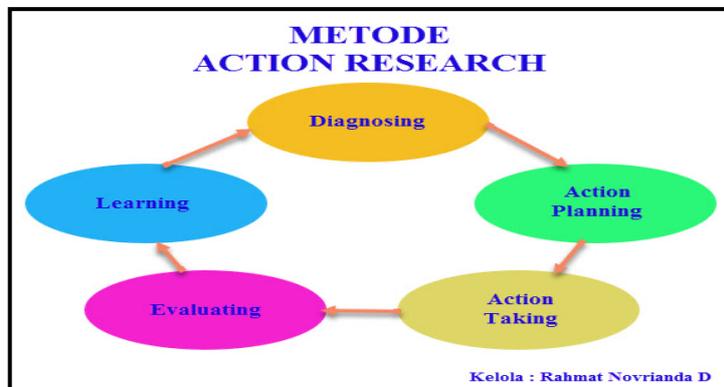
Pada penelitian ini akan diambil suatu kasus *cyber crime*, dalam hal ini adalah *cyberbullying*, dimana tindak kejahatan ini dilakukan melalui media sosial. Adapun media sosial ini adalah suatu wadah yang dipergunakan dalam proses interaksi ataupun komunikasi antar individu atau kelompok di dunia maya [7]. Adapun diperoleh hasil dari penelitian sebelumnya bahwa Teknik Digital Forensik juga pernah digunakan dalam menganalisis bukti digital dari media sosial *Twitter* [8]. Oleh karena itu, pada penelitian ini juga memanfaatkan media sosial yang sering digunakan oleh masyarakat. Adapun dari hasil survei pada tahun 2017, diperoleh 2 media sosial yang memiliki pesan instan yang paling sering digunakan, yaitu *Facebook Messenger* dengan hasil survei 77,26 % dan *Whatsapp* sebanyak 97,24 % dari seluruh responden dari berbagai kalangan [9]. Penelitian ini berfokus terhadap bukti digital dari pesan instan pada kedua media sosial tersebut yang telah terhapus ataupun sengaja dihapus, yang mana pesan instan adalah media komunikasi yang memfasilitasi masyarakat dalam perkembangan IoT untuk berkomunikasi secara *real time* dalam bentuk tulisan, gambar, suara ataupun video [10]. Terdapat 2 media sosial dengan pesan instan yang digunakan pada penelitian ini, yaitu *Facebook Messenger* yang merupakan fasilitas pesan instan yang diluncurkan *Facebook* pada tahun 2008 [11] dan *Whatsapp* yang merupakan *software* pesan instan yang dapat dioperasikan pada *smartphone* yang menggunakan berbagai jenis *platform* [12].

Pada penelitian dengan menggunakan Metode *Action Research* ini, peneliti mengambil kasus dimana bukti digital berkaitan dengan *cyber crime* yang telah terhapus dari aplikasi pesan instan *Facebook Messenger* dan *Whatsapp*. Dengan menerapkan Teknik Digital Forensik, penulis akan memperoleh dokumentasi dari setiap tahapan dalam proses pengungkapan bukti

digital yang telah terhapus [13]. *Cyber crime* yang diambil dalam penelitian ini adalah *cyberbullying* melalui pesan instan media sosial, yang mana *cyberbullying* hanyalah contoh kecil dari tindak kejahatan di dunia maya. Oleh karena itu, hasil dari penelitian yang dilakukan ini juga dapat diterapkan terhadap pengungkapan bukti digital dari *cyber crime* lainnya yang dilakukan melalui *Facebook Messenger* dan *Whatsapp*. Tidak hanya terbatas pada *cyber crime*, hasil dari penelitian ini juga dapat diterapkan dalam mengungkapkan bukti digital lain yang telah terhapus dari *Facebook Messenger* dan *Whatsapp*.

2. METODE PENELITIAN

Agar proses penelitian dapat berjalan secara runtut, maka diperlukan adanya metode penelitian yang memiliki tahapan penelitian yang jelas, yang mana pada penelitian ini digunakan Metode *Action Research*. Adapun metode ini merupakan suatu rancangan tahapan penelitian yang dapat menjelaskan serta menggambarkan kondisi untuk tujuan penyempurnaan [14]. Gambar 1 berikut ini merupakan tahapan dari metode penelitian *action research* [15]:



Gambar 1 Metode *Action Research* [16]

2.1 *Diagnosing*

Pada tahapan ini, peneliti melakukan survei dari beberapa hasil penelitian terdahulu serta beberapa pemberitaan terkait dengan *Cyber Crime*, terutama pada kasus Tindakan Ancaman ataupun *Bullying* yang memanfaatkan Media Sosial. Dari data yang diperoleh, kasus Tindakan Ancaman ataupun *Bullying* banyak terjadi di kalangan remaja. Selain itu, media sosial yang marak digunakan masyarakat adalah *Facebook Messenger* dan *Whatsapp*. Oleh karena itu, bukti digital saat ini telah valid untuk mengungkap suatu kejahatan tepatnya *cyber crime*. Akan tetapi, kebanyakan bukti digital ini hilang karena terhapus ataupun sengaja dihapus dari *history* aplikasinya.

2.2 *Action Planning*

Setelah melakukan survei, peneliti merancang suatu rencana untuk memberikan pemecahan masalah yang tepat. Adapun permasalahan yang terjadi adalah kehilangan bukti digital yang berupa *history* percakapan pada Pesan Instan, dimana pada penelitian ini diambil contoh *Facebook Messenger* dan *Whatsapp*. Oleh karena itu, peneliti membuat suatu skenario percakapan yang berisikan Tindakan Ancaman ataupun *Bullying*, setelah itu bukti-bukti percakapan tersebut sengaja dihapus. Kemudian, peneliti membuat perencanaan tahapan Digital Forensik terhadap media penyimpanan yang sebelumnya digunakan untuk mengakses *Facebook Messenger* dan *Whatsapp* untuk mengungkap bukti-bukti yang telah terhapus. Adapun pada penelitian ini, digunakan beberapa bukti digital seperti *text*, gambar dan video berkaitan dengan *cyberbullying* yang dikirimkan melalui *Facebook Messenger* dan *Whatsapp*. Berikut ini secara berturut-turut bukti digital yang digunakan yaitu skenario percakapan (Gambar 2), gambar (Gambar 3) dan video (Gambar 4) yang berisikan *bullying* :

```
a : hei jelek
b : iya ada apa
a : kerjakan prku
b : kenapa harus aku
a : kerjakan atau akan ku kirim poto jelekmu ke sosmed( mengirim poto)
b : jangan aku malu
a : makanya kerjakan prku
b : iya baiklah nanti aku kerjakan
a : nah gitu dong
b : iya, kenapa harus aku
a : ehh kamu gotot yah jelek
b : enggak cuma nanya
a : kamu awas yah aku sebar video kamu di bully kemaren
b : jangan maaf
a : aku kirim videonya ( mengirim video )
b : tolong jangan di kirim, maaf
```

Gambar 2 Skenario Percakapan *Facebook Messenger* dan *Whatsapp*

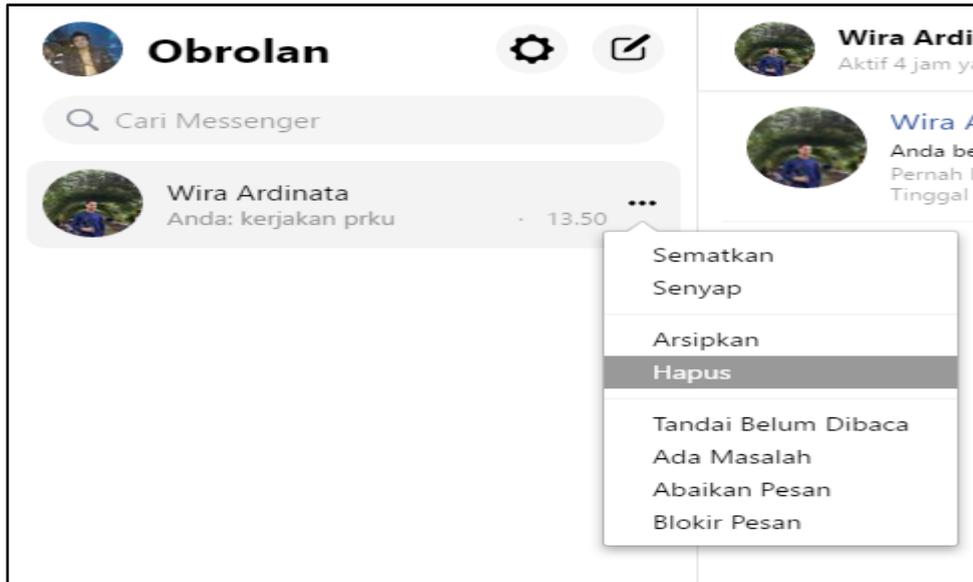


Gambar 3 Bukti Gambar tindakan *cyberbullying* pada *Facebook Messenger* dan *Whatsapp*

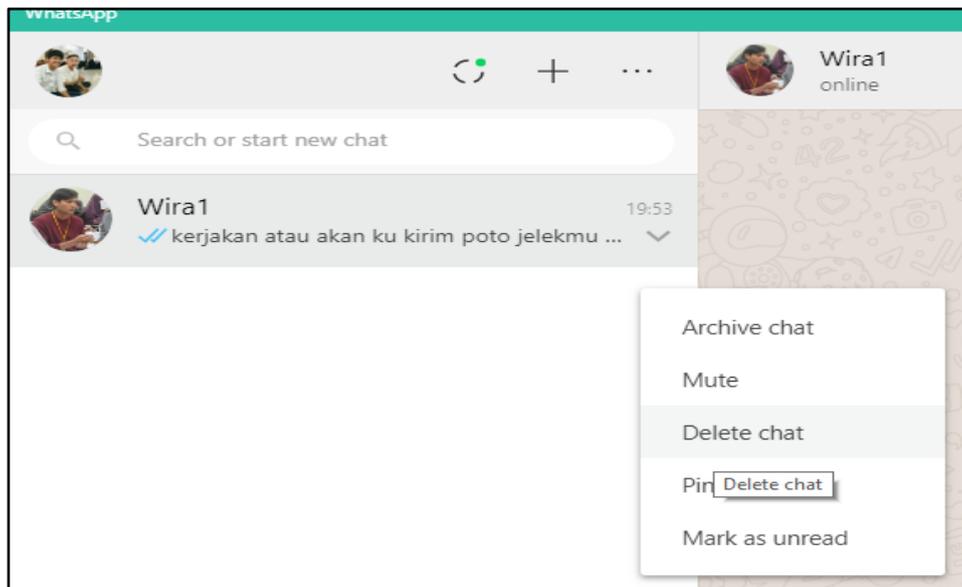


Gambar 4 Potongan video *cyberbullying* pada *Facebook Messenger* dan *Whatsapp*

Perencanaan selanjutnya adalah menghapus percakapan yang telah dikirimkan pada *Facebook Messenger* dan *Whatsapp*, yang mana hal ini menggambarkan suatu kasus disaat bukti digital terhapus ataupun sengaja dihapus, sehingga pada tahapan penelitian berikutnya dilakukan proses Digital Forensik untuk mengungkapkan bukti-bukti kejahatan di dunia maya yang telah terhapus (*Deleted Cyber Crime Evidence*). Berikut ini proses penghapusan percakapan pada *Facebook Messenger* dan *Whatsapp* secara berturut-turut pada Gambar 5 dan Gambar 6.



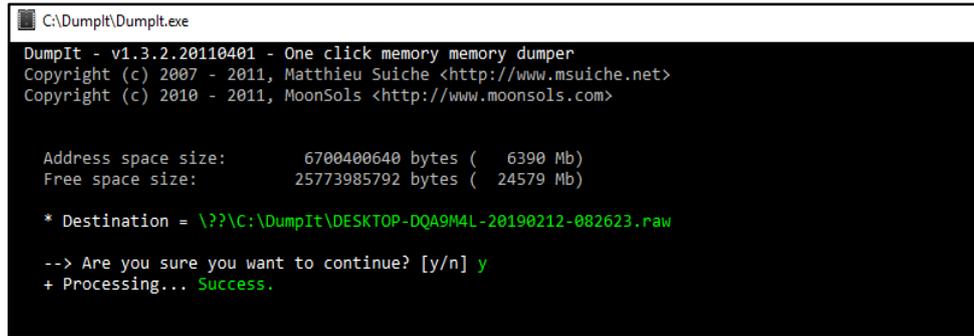
Gambar 5 Penghapusan Percakapan *Cyberbullying* pada *Facebook Messenger*



Gambar 6 Penghapusan Percakapan *Cyberbullying* pada *Whatsapp*

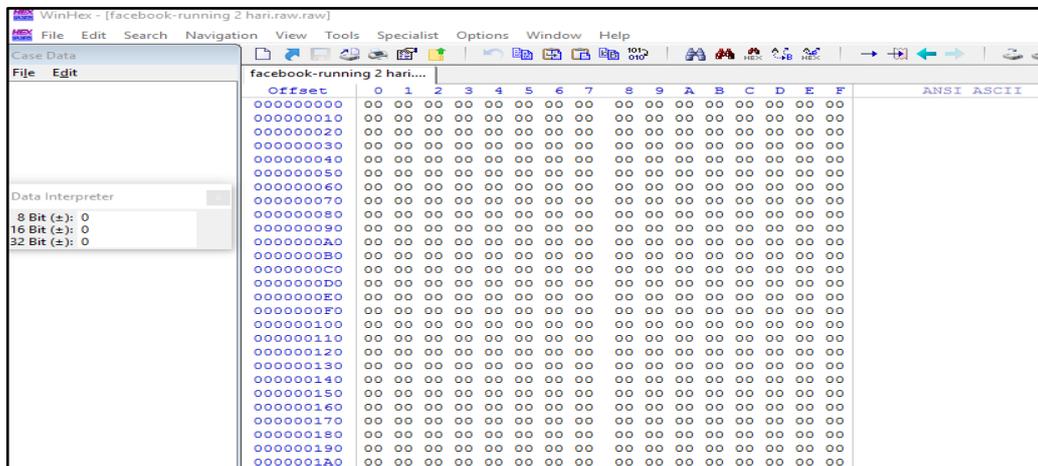
2.3 Action Taking

Setelah perencanaan dibuat serta skenario dirancang, maka pada tahapan ini peneliti mengeksekusi perangkat keras ataupun *Smartphone* yang digunakan untuk mengakses *Facebook Messenger* dan *Whatsapp* sebelumnya. Kemudian, dengan memanfaatkan beberapa *tools* Digital Forensik seperti *DumpIt*, peneliti mengambil kembali *history* yang telah berjalan pada *memory* ataupun RAM (*Random Access Memory*) dari perangkat keras atau *smartphone* yang digunakan untuk aplikasi *Facebook Messenger* dan *Whatsapp* dalam tindakan *cyberbullying* ini. Setelah itu, peneliti mulai melakukan analisis terhadap data-data temuan dengan memanfaatkan *tool* *Winhex*, yang mana data-data temuan dapat berupa *text*, gambar ataupun potongan gambar video. Berikut ini merupakan hasil dari proses *DumpIt* yang telah berhasil melakukan proses *dump* pada RAM dari perangkat keras atau *smartphone* yang digunakan dalam melakukan *cyberbullying*, dapat dilihat pada Gambar 7 di bawah ini :



Gambar 7 Proses dump telah berhasil menggunakan *DumpIt*.

Kemudian, untuk tahapan berikutnya dimanfaatkan *tool Winhex* untuk menemukan bukti-bukti digital dari *cyberbullying* yang telah terjadi, yang mana dapat diketahui bentuk *file* dari bukti digital tersebut apakah *text*, gambar atau video. Berikut ini pada Gambar 8, dapat dilihat tampilan dari *software Winhex* yang digunakan :



Gambar 8 Tampilan dari *tool Winhex*

WinHex merupakan suatu *software editor* yang menampilkan data dalam bentuk bilangan *hexadecimal*, yang sangat memberikan bantuan pada proses analisis forensik. Untuk memperoleh data yang dibutuhkan, peneliti harus mencari satu per satu dari keseluruhan bilangan *hexadecimal* yang tampil, tetapi akan lebih mudah mencari bukti digital yang dibutuhkan jika diketahui *userid* (ID Korban) ataupun *senderid* (ID Pelaku). Pada penelitian ini, kasus yang diteliti merupakan suatu skenario yang dirancang peneliti, sehingga peneliti mengetahui *userid* dan digunakan untuk mempercepat pencarian bukti digital dari *cyberbullying* yang telah terjadi.

2.4 Evaluating

Pada tahapan ini, peneliti melakukan evaluasi terhadap temuan-temuan yang ditemukan dimana dapat ditampilkan menggunakan *tool Winhex*. Secara detail dapat dijelaskan oleh peneliti untuk masing-masing data temuan yang berkaitan dengan bukti Tindakan Ancaman ataupun *Bullying* tersebut. Selain itu, peneliti juga melakukan evaluasi terhadap proses Digital Forensik yang telah dilakukan agar dapat dikomersialisasikan sebagai suatu Teknik yang dapat membantu proses pengungkapan bukti digital dari *cyber crime* khususnya serta bukti-bukti digital dalam kebutuhan lainnya pada umumnya.

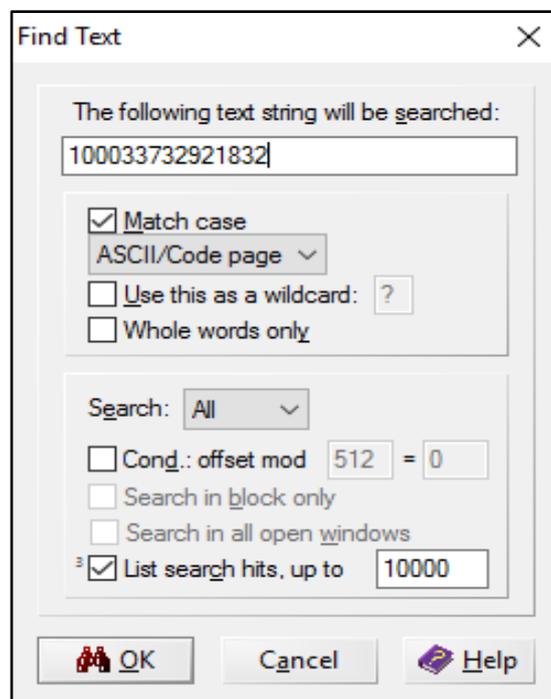
2.5 Learning

Tahapan ini merupakan tahapan akhir dari Metode Penelitian, dimana pada tahapan ini peneliti melakukan Pembelajaran lebih terhadap Teknik Digital Forensik yang diterapkan. Selain itu, penulis juga mempelajari ciri-ciri dari bukti digital yang ditemukan dengan proses Teknik Digital Forensik, apakah buktinya berbentuk *text* / tulisan, *file* gambar atau bahkan *file* video.

3. HASIL DAN PEMBAHASAN

Penelitian ini dilakukan untuk mengungkap bukti digital pada Pesan Instan dari Media Sosial yang terhapus ataupun sengaja dihapus. Oleh karena itu, dengan memanfaatkan beberapa *tools* Digital Forensik, peneliti dapat menentukan bentuk *file* apa saja dari bukti digital tindak *cyberbullying* yang dapat ditemukan. Adapun pada Gambar 2 telah diperlihatkan skenario percakapan *cyberbullying*, yang mana terdapat *text*, gambar dan juga video serta kemudian percakapan tersebut sengaja dihapus dari *Facebook Messenger* dan *Whatsapp*. Oleh karena itu, pada penelitian ini, dilakukan *dump* terhadap RAM dari *Smartphone* Korban *Cyberbullying* menggunakan *tool DumpIt* sehingga menghasilkan *file* berekstensi *raw* (.*raw*) yang dapat dilihat pada Gambar 7.

Setelah itu, *file* hasil *dump* tersebut dibuka dan dianalisis menggunakan *tool Winhex*. Untuk mempermudah dan mempercepat pencarian bukti digital dari *cyberbullying*, maka dilakukan pencarian menggunakan *userid* (ID Korban). Adapun pada penelitian ini telah diketahui *userid* pada *Facebook Messenger* adalah 100033732921832 dan *userid* pada *Whatsapp* adalah 165901725. Berikut ini merupakan proses pencarian serta hasil pencarian pada *tool Winhex*, yang mana pada Gambar 9 dan Gambar 10 merupakan proses pencarian dan hasil pencarian untuk *userid Facebook Messenger* serta pada Gambar 11 dan Gambar 12 adalah proses pencarian dan hasil pencarian untuk *userid Whatsapp*.



Gambar 9 Proses pencarian *userid Facebook Messenger*

hari.raw.raw]

tion View Tools Specialist Options Window Help

facebook-running 1 hari....

Position Manager (General)

Offset ▲	Search hits	Time
2B40D9	100033732921832	07/08/2019 13:37:12
2B4179	100033732921832	07/08/2019 13:37:12
2B4194	100033732921832	07/08/2019 13:37:12
2B4231	100033732921832	07/08/2019 13:37:12
2B42D2	100033732921832	07/08/2019 13:37:12
2B42ED	100033732921832	07/08/2019 13:37:12
2B4389	100033732921832	07/08/2019 13:37:12
2B442A	100033732921832	07/08/2019 13:37:12
2B4445	100033732921832	07/08/2019 13:37:12
2B44E1	100033732921832	07/08/2019 13:37:12
2B4582	100033732921832	07/08/2019 13:37:12
2B459D	100033732921832	07/08/2019 13:37:12
359B9E	100033732921832	07/08/2019 13:37:12
359FAE	100033732921832	07/08/2019 13:37:12
50319E	100033732921832	07/08/2019 13:37:12

Gambar 10 Hasil pencarian *userid Facebook Messenger*

Find Text

The following text string will be searched:

165901725]

Match case
 ASCII/Code page ▾

Use this as a wildcard: ?

Whole words only

Search: All ▾

Cond.: offset mod 512 = 0

Search in block only

Search in all open windows

List search hits, up to 10000

OK Cancel Help

Gambar 11 Proses pencarian *userid Whatsapp*

Offset ▲	Search hits	Time
1CAD48D	165901725	07/08/2019 14:19:28
9F6E167	165901725	07/08/2019 14:19:28
19537AF9	165901725	07/08/2019 14:19:28
1A54F097	165901725	07/08/2019 14:19:28
1C007427	165901725	07/08/2019 14:19:28
20C21CD3	165901725	07/08/2019 14:19:28
253790CA	165901725	07/08/2019 14:19:28
3A98C335	165901725	07/08/2019 14:19:28
3D81F771	165901725	07/08/2019 14:19:28
3FFCF347	165901725	07/08/2019 14:19:28
407358A1	165901725	07/08/2019 14:19:28
41A27DCF	165901725	07/08/2019 14:19:28
4C2CFD0D	165901725	07/08/2019 14:19:28
55A02AE5	165901725	07/08/2019 14:19:28
5664716D	165901725	07/08/2019 14:19:28

Gambar 12 Hasil pencarian *userid* *Whatsapp*

Setelah diperoleh hasil dari pencarian *userid* pada *Facebook Messenger* dan *Whatsapp*, maka peneliti melakukan penelusuran untuk mencari dan menemukan bentuk file bukti - bukti *cyberbullying* yang terlihat melalui *tool Winhex* seperti pada gambar-gambar di bawah ini. Adapun berturut-turut penemuan bukti dalam bentuk *text* / tulisan, *file* gambar dan video dari *Facebook Messenger* disajikan pada Gambar 13, 14 dan 15. Selain itu, penemuan bukti dalam bentuk *text* / tulisan dan *file* video dari *Whatsapp* disajikan pada Gambar 16 dan 17.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
09CA73DD0	65	75	65	45	6E	74	69	74	79	49	64	22	3A	31	30	30	eueEntityId":100
09CA73DE0	30	33	33	37	33	32	39	32	31	38	33	32	7D	D0	00	D0	033732921832}D D
09CA73DF0	00	D0	D D D D D D D D														
09CA73E00	00	D0	00	D0	00	D0	00	32	F5	03	00	05	2F	74	5F	6D	D D D 2d /t_m
09CA73E10	73	0E	37	7B	22	64	65	6C	74	61	73	22	3A	5B	7B	22	s 7{"deltas":[{"
09CA73E20	61	74	74	61	63	68	6D	65	6E	74	73	22	3A	5B	5D	2C	attachments":[],
09CA73E30	22	62	6F	64	79	22	3A	22	68	65	69	20	6A	65	6C	65	"body":"hei jele
09CA73E40	6B	22	2C	22	69	72	69	73	53	65	71	49	64	22	3A	22	k","irisSeqId":
09CA73E50	37	22	2C	22	6D	65	73	73	61	67	65	4D	65	74	61	64	7","messageMetad
09CA73E60	61	74	61	22	3A	7B	22	61	63	74	6F	72	46	62	49	64	ata":{"actorFbId
09CA73E70	22	3A	22	31	30	30	30	33	33	37	33	32	39	32	31	38	":"1000337329218
09CA73E80	33	32	22	2C	22	6D	65	73	73	61	67	65	49	64	22	3A	32","messageId":
09CA73E90	22	6D	69	64	2E	24	63	41	41	41	41	43	52	4C	71	6C	"mid.\$cAAAACRLq1
09CA73EA0	47	5A	76	45	6C	6F	63	58	56	6F	34	55	78	43	6C	5A	GZvElocXVo4UxC1Z
09CA73EB0	58	6B	4F	22	2C	22	6F	66	66	6C	69	6E	65	54	68	72	XkO","offlineThr
09CA73EC0	65	61	64	69	6E	67	49	64	22	3A	22	36	35	30	31	30	earingId":"65010
09CA73ED0	33	37	33	39	33	30	36	38	37	38	33	38	38	36	22	2C	37393068783886",

Gambar 13 Penemuan bukti *cyberbullying* dalam bentuk *Text* / Tulisan dari *Facebook Messenger*

6F 3F 01 53 04 74 79 70-65 3F 01 53 07 6D 65 73	0? -S-type? -S-mes
73 61 67 65 3F 01 53 07-6D 65 73 73 61 67 65 3F	sage? -S-message?
01 6F 3F 02 53 04 62 6C-6F 62 3F 02 66 14 45 3A	-o? -S-blob? -f-E:
5C 6B 65 6E 61 62 75 6C-69 20 6B 61 6D 75 2E 6A	\kenabuli kamu.j
70 67 11 6B 65 6E 61 62-75 6C 69 20 6B 61 6D 75	pg,kenabuli kamu
2E 6A 70 67 00 24 35 66-63 39 39 30 61 65 2D 66	.jpg-\$5fc990ae-f
35 36 39 2D 34 63 61 33-2D 61 61 66 38 2D 31 33	569-4ca3-aaf8-13
33 64 35 64 33 35 63 36-64 64 0A 69 6D 61 67 65	3d5d35c6dd-image
2F 6A 70 65 67 00 01 3F-03 53 06 68 65 69 67 68	/jpeg-? -S-heigh
74 3F 03 49 80 20 3F 03-53 05 77 69 64 74 68 3F	t? -I- ? -S-width?
03 49 80 20 3F 03 53 07-71 75 61 6C 69 74 79 3F	-I- ? -S-quality?
03 49 AA 01 3F 03 53 0A-75 6E 64 65 72 73 68 6F	-I+ -? -S-undersho
6F 74 3F 03 49 00 7B 05-7B 02 00 00 01 00 00 00	ot? -I-{: { - - - - -
31 DD 01 00 05 2F 74 5F-6D 73 7B 22 64 65 6C 74	1Y-.../t_ms{"delt
61 73 22 3A 5B 7B 22 69-72 69 73 53 65 71 49 64	as": [{"irisSeqId
22 3A 22 33 30 32 22 2C-22 72 65 71 75 65 73 74	": "302", "request
43 6F 6E 74 65 78 74 22-3A 7B 22 61 70 69 41 72	Context": {"apiAr
67 73 22 3A 7B 7D 7D 2C-22 74 68 72 65 61 64 4B	gs": {}}, "threadK
65 79 73 22 3A 5B 7B 22-6F 74 68 65 72 55 73 65	ey": [{"otherUse
72 46 62 49 64 22 3A 22-31 30 30 30 30 33 39 31	rFbId": "10000391
37 32 39 30 38 39 34 22-7D 5D 2C 22 63 6C 61 73	7290894"}], "clas
73 22 3A 22 54 68 72 65-61 64 44 65 6C 65 74 65	s": "ThreadDelete
22 7D 5D 2C 22 66 69 72-73 74 44 65 6C 74 61 53	"}], "firstDeltaS
65 71 49 64 22 3A 33 30-32 2C 22 6C 61 73 74 49	eqId": 302, "lastI
73 73 75 65 64 53 65 71-49 64 22 3A 33 30 32 2C	ssuedSeqId": 302,
22 71 75 65 75 65 45 6E-74 69 74 79 49 64 22 3A	"queueEntityId":
31 30 30 30 33 33 37 33-32 39 32 31 38 33 32 7D	100033732921832}
56 6E 4A 80 00 00 00 00-16 03 00 00 48 02 00 00	VnJ- - - - -H- - -
00 00 00 00 00 00 00 00-16 03 00 00 48 02 00 00	- - - - -H- - -
00 00 00 00 00 00 00 00-16 03 00 00 48 02 00 00	- - - - -H- - -

Gambar 14 Penemuan bukti *cyberbullying* dalam bentuk Gambar dari *Facebook Messenger*

05789E9B0	38 74 72 67 26 6A 61 7A 6F 65 73 74 3D 32 38 30	8trg&jazoest=280
05789E9C0	35 35 69 64 69 6D 6D 3B 2F 70 38 41 63 70 38 41	55idimm;/p8Acp8A
05789E9D0	45 44 63 73 4D 46 31 64 00 00 00 00 00 00 00 80	EDcsMFid €
05789E9E0	51 00 26 00 00 50 D9 40 00 00 00 00 00 00 00 80	Q & PÜ€ €
05789E9F0	4A 00 27 00 00 20 E2 40 00 00 00 00 00 00 00 80	J ' ä@ €
05789EA00	30 87 4C 80 28 3B 3B 29 3B 7B 22 5F 5F 61 72 22	0+L€(;;);{"__ar"
05789EA10	3A 31 2C 22 70 61 79 6C 6F 61 64 22 3A 7B 22 75	:1, "payload": {"u
05789EA20	70 6C 6F 61 64 49 44 22 3A 6E 75 6C 6C 2C 22 6D	ploadID": null, "m
05789EA30	65 74 61 64 61 74 61 22 3A 5B 7B 22 76 69 64 65	etadata": [{"vide
05789EA40	6F 5F 69 64 22 3A 31 38 33 33 30 30 39 39 30 30	o_id": 1833009900
05789EA50	31 34 34 33 33 32 2C 22 66 69 6C 65 6E 61 6D 65	144332, "filename
05789EA60	22 3A 22 6B 61 6D 75 20 74 65 72 73 61 6B 69 74	": "kamu tersakit
05789EA70	69 2E 4D 50 34 22 2C 22 66 69 6C 65 74 79 70 65	i.MP4", "filetype
05789EA80	22 3A 22 76 69 64 65 6F 5C 2F 6D 70 34 22 2C 22	": "video/mp4",
05789EA90	74 68 75 6D 62 6E 61 69 6C 5F 73 72 63 22 3A 22	thumbnail_src": "
05789EA90	68 74 74 70 73 33 5C 3F 5C 3F 73 63 6F 6F 74 65	https://(scante

Gambar 15 Penemuan bukti *cyberbullying* dalam bentuk Video dari *Facebook Messenger*

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
104906150	E1	A4	6B	A6	D0	41	D8	82	EA	7B	B8	A2	C6	C4	2B	0F	á×k;DA0,ê{,cEÄ+
104906160	01	30	51	62	05	10	EA	34	38	20	F0	E3	B7	69	45	44	0Qb ê48 ðä-iED
104906170	A3	6C	B6	43	36	60	72	A1	CA	6F	9E	12	38	23	D2	E4	£1QC6`r;Ëož 8#0ä
104906180	00	00	48	C9	77	14	C3	00	31	36	35	39	30	31	37	32	HÉw Ä 16590172
104906190	35	40	73	2E	77	68	61	74	73	61	70	70	2E	6E	65	74	5@s.whatsapp.net
1049061A0	10	01	1A	14	33	45	42	30	32	42	35	35	37	32	41	33	3EB02B5572A3
1049061B0	38	36	36	41	33	35	30	35	12	18	0A	16	6D	61	6B	61	866A3505 maka
1049061C0	6E	79	61	20	6B	65	72	6A	61	6B	61	6E	20	70	72	20	nya kerjakan pr
1049061D0	6B	75	18	D8	B1	90	E3	05	20	01	90	E3	05	20	00	00	ku 0± ä ä

Gambar 16 Penemuan bukti *cyberbullying* dalam bentuk *Text / Tulisan* dari *Whatsapp*

00EAF3980	F1 62 DD 6E 5B 32 30 3A 31 35 2C 20 32 2F 31 33	ñbÿn[20:15, 2/13
00EAF3990	2F 32 30 31 39 5D 20 57 69 72 61 3A 20 00 62 00	/2019] Wira: b
00EAF39A0	01 00 00 00 15 00 00 00 00 00 00 69 45 3A 5C 6B	iE:\x
00EAF39B0	61 6D 75 20 74 65 72 73 61 6B 69 74 69 2E 4D 50	amu tersakiti.MP
00EAF39C0	34 69 6E 67 75 00 00 00 40 2A A2 D2 87 1A 00 00	4ingu @*ç0#
00EAF39D0	90 25 A2 D2 87 1A 00 00 98 32 A2 D2 87 1A 00 00	%ç0# 2*ç0#
00EAF39E0	C0 EC A1 D2 87 1A 00 00 D0 09 A2 D2 87 1A 00 00	Àì;0# Ð ç0#
00EAF39F0	00 00 63 B2 0A 63 5E F0 04 00 00 00 00 00 00 00	c^ c^8
00EAF3A00	E0 10 43 76 05 4E 00 00 C0 FF FF FF 00 00 00 00	à Cv N Àÿÿÿ
00EAF3A10	00 00 00 00 87 1A 00 00 01 00 00 00 1A 00 00 00	#

Gambar 17 Penemuan bukti cyberbullying dalam bentuk Video dari Whatsapp

Dari hasil penelusuran yang diperoleh pada Gambar 13 hingga Gambar 17, dapat dijelaskan bahwa dengan menggunakan *software WinHex* dapat ditemukan ataupun dideteksi adanya bukti digital dengan bentuk *text*, *file* gambar dan video dari *userid Facebook Messenger* dan dideteksi adanya bentuk *text* dan *file* video dari *userid Whatsapp*. Adapun dari Gambar 13 dapat dilihat terdeteksi potongan *text* dengan isi “hei jelek” dan Gambar 16 dapat dilihat dideteksi tulisan ”makanya kerjakan pr ku” yang merupakan bukti digital *cyberbullying* dalam bentuk *text* / tulisan. Selain itu, pada Gambar 14 dapat dilihat terdapat tulisan nama *file* dengan ekstensi *.jpg* yang merupakan bukti digital dalam bentuk *file* gambar. Kemudian berikutnya, pada Gambar 15 dan Gambar 17 terdapat tulisan *file* berekstensi *.MP4* yang merupakan salah satu bentuk ekstensi dari *file* video. Berikut ini peneliti sajikan rangkuman hasil pengungkapan ataupun penemuan bukti digital dengan Teknik Digital Forensik yang peneliti gunakan, dapat dilihat pada Tabel 1 di bawah ini:

Tabel 1 Penemuan bukti digital dari pesan instan media sosial

Pesan Instan Media Sosial	Bentuk Bukti Digital		
	Text	Gambar	Video
Facebook Messenger	Ditemukan	Ditemukan	Ditemukan
Whatsapp	Ditemukan	Tidak Ditemukan	Ditemukan

Dari Tabel 1 di atas, dapat dilihat bahwa dari penelusuran menggunakan *userid Facebook Messenger* ditemukan seluruh bentuk bukti digital yang dikirimkan sesuai skenario percakapan yaitu terdapat *text* / tulisan, gambar dan video. Akan tetapi, dari hasil penelusuran *userid Whatsapp* terdapat 1 bentuk *file* yang tidak ditemukan yaitu *file* gambar, yang mana hal ini dapat terjadi dikarenakan saat proses *dump* dari RAM perangkat *mobile* atau *smartphone* yang tidak sempurna atau bisa disebabkan karena fungsi RAM pada penyimpanan *history* data untuk *Whatsapp* tidak lagi bekerja dengan optimal. Selain itu, pada Tabel 2 berikut ini disajikan data perbedaan temuan antara bukti digital *text*, gambar maupun video.

Tabel 2 Perbedaan temuan bukti digital *text*, *file* gambar dan video

Bukti Digital	Ciri-Ciri
Text / Tulisan	Terlihat adanya potogan <i>text</i> / tulisan. - Pada penelusuran <i>userid Facebook Messenger</i> terlihat potongan <i>text</i> “hei jelek” - Pada penelusuran <i>userid Whatsapp</i> terlihat potongan <i>text</i> “makanya kerjakan pr ku”
Gambar	Terlihat tulisan dengan ekstensi “.jpg” atau “.jpeg”
Video	Terlihat tulisan dengan ekstensi “.MP4”

Text / tulisan serta *file* gambar dan video ini merupakan isi dari skenario percakapan yang telah peneliti rancang serta sengaja dihapus untuk dijadikan suatu kasus sehingga Teknik Digital Forensik yang peneliti lakukan pada penelitian ini dapat digunakan dalam pengungkapan ataupun penemuan bukti-bukti digital yang terhapus pada kasus lainnya terutama bukti dari pesan instan *Facebook Messenger* dan *Whatsapp*. Adapun syarat utama dalam melakukan

Teknik Digital Forensik ini adalah memiliki ataupun menemukan Perangkat *Mobile* ataupun *Smartphone* yang digunakan dalam tindakan *bullying* atau *cyberbullying*, ataupun dalam tindakan dan kasus lainnya.

Dari hasil penelitian yang telah dilakukan, dapat dijelaskan bahwa Teknik Digital Forensik yang diterapkan pada penelitian ini dapat mengidentifikasi beberapa jenis bukti-bukti digital seperti text, gambar dan potongan video. Adapun jenis bukti-bukti digital ini dapat dibedakan dengan melihat jenis ekstensi yang terlihat pada source code yang telah diterjemahkan dari bentuk bilangan hexadesimal menggunakan tools Winhex. Selain itu, dapat dilihat juga kata kunci dari bukti digital yang dibutuhkan melalui jendela tool Winhex, seperti potongan percakapan (text), nama file gambar yang berkaitan dengan bukti digital yang dibutuhkan (gambar) dan nama file video (video). Adapun pada penelitian ini, contoh kasus yang diambil adalah cyberbullying, maka file yang kata kuncinya berkaitan dengan bullying yang diidentifikasi. Adapun kata kunci yang berkaitan dengan cyberbullying dapat dilihat pada Gambar 14, 15 dan 16.

4. KESIMPULAN DAN SARAN

Dari hasil penelitian yang telah dilakukan dalam pengungkapan adanya bukti *cyberbullying* dengan Teknik Digital Forensik, maka dapat ditarik beberapa kesimpulan sebagai berikut:

1. Teknik Digital Forensik untuk mengungkap adanya bukti digital dilakukan dengan *dump* pada RAM, sehingga dibutuhkan Perangkat *Mobile* ataupun *Smartphone* yang menjadi barang bukti fisik.
2. Bukti *cyberbullying* sesuai dengan skenario percakapan yang berisi *text*, *file* gambar dan video tetap dapat ditemukan walaupun percakapan telah terhapus ataupun sengaja dihapus, karena *history* kerja aplikasi ataupun *software* Facebook Messenger dan Whatsapp masih tersimpan pada RAM.
3. Kemungkinan bukti digital tidak ditemukan masih bisa terjadi, yang mana hal ini disebabkan oleh proses *dump* yang kurang sempurna ataupun terdapat kerusakan atau *bad sector* pada RAM dari Perangkat *Mobile* / *Smartphone* yang menjadi bukti fisiknya.

UCAPAN TERIMA KASIH

Ucapan terima kasih disampaikan kepada Universitas Bina Darma yang telah memberikan dana Penelitian Internal untuk skim Penelitian Multi Disiplin Ilmu. Selain itu, diucapkan juga terima kasih kepada Mahasiswa Universitas Bina Darma yang telah memberikan bantuan dalam pengumpulan data dan proses penyelesaian penelitian ini. Ucapan terima kasih yang sebesar - besarnya kepada Tim Redaksi Jurnal Techno.COM yang telah mempublikasikan hasil penelitian ini.

DAFTAR PUSTAKA

- [1] M. Rifauddin, "Fenomena Cyberbullying pada Remaja (Studi Analisis Media Sosial Facebook)," *J. Ilmu Perpustakaan, Inf. dan Kearsipan Khizanah Al-Hikmah*, vol. 4, no. 1, pp. 35–44, 2016.
- [2] I. Rahmawati, "Analisis Manajemen Risiko Ancaman Kejahatan Siber," *J. Pertahanan Bela Negara*, vol. 7, no. 2, pp. 51–66, 2017.
- [3] E. Z. Zakiyah, S. Humaedi, and M. B. Santoso, "Faktor yang Mempengaruhi Remaja dalam melakukan Bullying," *J. Penelit. PPM*, vol. 4, no. 2, pp. 324–330, 2017.
- [4] N. Fahmi, E. Prayitno, and S. Fitriani, "Web of Thing Application for Monitoring Precision Agriculture Using Wireless Sensor Network," *J. INFOTEL (Informatika - Telekomun. - Elektron.*, vol. 11, no. 1, pp. 22–28, 2019.
- [5] I. N. Prawiranegara and G. H. A. Kusuma, "Analisa Digital Forensik Rekaman Video

- CCTV dengan Menggunakan Metadata dan Hash,” in *Prosiding SISFOTEK*, 2019, pp. 223–227.
- [6] N. Iman, A. Susanto, and R. Inggi, “Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review),” *InComTech J. Telekomun. dan Komput.*, vol. 9, no. 3, pp. 186–192, 2019.
- [7] A. Hermawansyah and A. R. Pratama, “Analisis Profil dan Karakteristik Pengguna Media Sosial di Indonesia Dengan Metode EFA dan MCA,” *Techno.COM*, vol. 20, no. 1, pp. 69–82, 2021.
- [8] I. Zuhriyanto, A. Yudhana, and I. Riadi, “Perancangan Digital Forensik Pada Aplikasi Twitter Menggunakan Metode Live Forensics,” 2018.
- [9] F. Zebua, “Laporan Daily Social: Survey Instant Messaging 2017,” 2017.
- [10] A. D. Nugroho and R. Munir, “Aplikasi Enkripsi Instant Messaging pada Perangkat Mobile dengan menggunakan Algoritma Elliptic Curve Cryptography (ECC),” in *KNIF 2015*, 2015, pp. 146–151.
- [11] A. Yudhana, I. Riadi, and I. Anshori, “Analisis Forensik Aplikasi Instant Messenger pada Smartphone berbasis Android,” *J. Insa. Comtech*, vol. 2, no. 2, pp. 25–31, 2017.
- [12] N. Anwar and I. Riadi, “Analisis Investigasi Forensik WhatsApp Messenger Smartphone terhadap WhatsApp berbasis Web,” *J. Ilmu Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, pp. 1–10, 2017.
- [13] M. N. Faiz, “Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal,” *J. Informatics, Inf. Syst. Softw. Eng. Appl.*, vol. 1, no. 1, 2018.
- [14] R. N. Dasmien, “Implementasi Raspberry Pi 3 sebagai Wireless Access Point pada STIPER Sriwigama Palembang,” *J. Inform. J. Pengemb. IT*, vol. 3, no. 3, pp. 387–393, 2018.
- [15] R. N. Dasmien and A. Khudri, “Optimasi Jaringan Wireless PT. TASPEN dengan RADIUS Server dan Firewall Filter Rules,” *Techno.COM*, vol. 20, no. 1, pp. 134–146, 2021.
- [16] R. N. Dasmien and Rasmila, “Implementasi Raspberry Pi 3 pada Sistem Pengontrol Lampu berbasis Raspbian Jessie,” *JEPIN (Jurnal Edukasi dan Penelit. Inform.)*, vol. 5, no. 1, pp. 46–53, 2019.