Investigasi Bukti Digital Aplikasi Wechat Menggunakan Framework Integrated Digital Forensics Proses Model (IDFPM) Berbasis SNI 27037:2014

Soni[1)], Eka Ramadhan[2)], dan Desti Mualfah[3)]
[1,2,3]Teknik Informatika, Universitas Muhammadiyah Riau
Jl. Tuanku Tambusai, Pekanbaru, Riau
e-mail: soni@umri.ac.id[1)], 150401035@student.umri.ac.id[2)], destimualfah@umri.ac.id[3)]

ABSTRAK

Media sosial menjadi sarana alternatif dalam sarana komunikasi pada Smartphone, Sebanyak 28% aplikasi instan messenger WeChat di gunakan sebagai interaksi sosial penyampaian pesan oleh pengirim dan penerimanya, adanya Cyberbullying pada aplikasi WeChat yang menghasilkan tindakan intimidasi yang dilakukan penggunanya, maka untuk menangani tindak kejahatan Cyberbullying aplikasi WeChat pada Smartphone dibutuhkan teknik Mobile Forensik untuk mengidentifikasi bukti digital percakapan verbal pada aplikasi WeChat menggunakan metode Framework Intergrated Digital Forensics Process Model (IDFPM) berbasis SNI 27037:2014 yang dilakukan pada Smartphone, Hasil dari penelitian ini berhasil mengidentifikasi artefak serta isi pesan percakapan Cyberbullying pada aplikasi WeChat yang sebelumnya terenkripsi dan nilai hashing md5 dan sha1 yang autentik, serta metadata atau timestamp pada pesan percakapan aplikasi WeChat menggunakan Tools Mobileedit Forensik Express, dan berhasil melakukan Penerapan Framework Integrated Digital Forensic Process Model (IDFPM) berbasis SNI 27037:2014 pada proses investigasi forensik dengan media Smartphone android.

***Kata Kunci** : Cyberbullying, WeChat, Mobile Forensik, Framework (IDFPM) berbasis SNI 27037:2014*

ABSTRACT

Social media is an alternative means of communication on smartphones, as many as 28% of the WeChat instant messenger application is used as a social interaction for the delivery of messages by senders and recipients, Cyberbullying on the WeChat application results in intimidation by users, so to deal with the crime of Cyberbullying applications WeChat on Smartphones requires a Mobile Forensic technique to identify digital evidence of verbal conversations on the WeChat application using the Framework Integrated Digital Forensics Process Model (IDFPM) method based on SNI 27037: 2014 which is carried out on Smartphones. WeChat application which was previously encrypted and hashing values of md5 and sha1 are authentic, as well as metadata or timestamp in the WeChat application conversation messages using the Mobileedit Forensic Express Tools, and successfully implemented Frame Work Integrated Digital Forensic Process Model (IDFPM) based on SNI 27037: 2014 on the forensic investigation process using Android Smartphone media.

***Keywords**: Cyberbullying, WeChat, Mobile Forensics, Framework (IDFPM) based on SNI 27037: 2014*

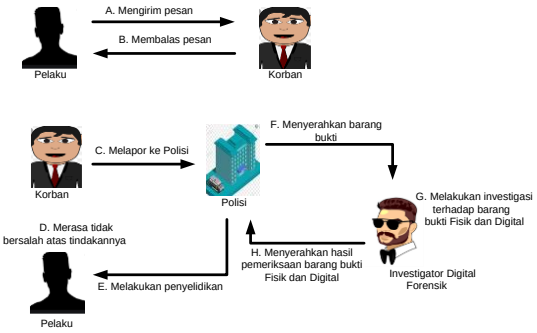
I. PENDAHULUAN

Perkembangan media elektronik di Indonesia berkembang dengan sangat pesat, indonesia merupakan salah satu negara dengan pengguna media sosial perangkat elektronik paling atraktif di dunia. Jumlah pengguna aktif media sosial di Indonesia pada januari 2019 mencapai 150 juta pengguna aktif media social, 130 juta diantaranya mengakses media sosial menggunakan Smartphone. Perkembangan pesat media sosial sebagai media komunikasi dua arah ini menunjukkan pengguna memperoleh dampak yang diharapkan dengan membuat akun dan berinteraksi di dalamnya. Salah satunya yaitu menggunakan aplikasi WeChat untuk sarana berkomunikasi, [1]. hasil riset Polling Indonesia yang bekerja sama dengan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mengatakan ada sekitar 49 persen netizen yang pernah menjadi sasaran bullying di media social, 3,6% diantaranya melaporkan ke pihak berwajib. [2] Adanya Cyberbullying yang berujung pada ancaman di media sosial yang terhubung dengan aplikasi WeChat yang akan menghasilkan tindakan kekerasan yang dilakukan penggunanya menjadikan suatu permasalahan di dalam ranah hukum serta merugikan korban, maka untuk menangani tindak kejahatan Cyberbullying aplikasi WeChat pada Smartphone dibutuhkan teknik Mobile Forensik untuk mengidentifikasi bukti digital percakapan verbal pada aplikasi WeChat menggunakan metode Framework Intergrated Digital Forensics Process Model (IDFPM) berbasis SNI 27037:2014 yang dilakukan pada Smartphone, [3]. Mobile Forensik adalah ilmu untuk memulihkan bukti digital dari perangkat Mobile dibawah kondisi forensik menggunakan metode yang diterima, [4].

Media sosial adalah aplikasi interaktif berbasis Internet, merupakan produk dari revolusi informasi yang berkembang pesat dalam dekade terakhir, yang telah mengubah cara komunikasi orang dan mengelola informasi

yang mengalir. WeChat adalah perangkat lunak aplikasi mobile, aplikasi WeChat memiliki serangkaian fitur cerdas dan keren, lengkap termasuk penggunaan Web WeChat, fitur ini membuat aplikasi ini berbeda dari aplikasi lain karena memungkinkan pengguna untuk mengobrol di komputer dan di ponsel, [5].

Tujuan dari penelitian ini adalah menjelaskan proses penanganan bukti digital sebuah percakapan verbal pada aplikasi WeChat, serta mencari artefak dan metadata suatu bukti digital dari barang bukti elektronik berupa Smartphone atas kejahatan berupa ancaman di media sosial pada aplikasi WeChat. Adapun rekayasa skenario pada penelitian ini dapat dilihat pada gambar 1 berikut :

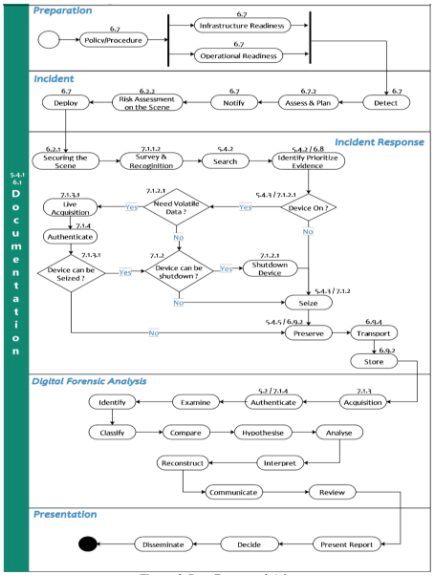


Gambar 1. Skenario Kasus *Cyberbullying*

Dari gambar diatas dapat dijelaskan Pelaku mengirim percakapan *Cyberbullying* secara verbal yang berisi pesan intimidasi kepada korban , Korban membalas pesan yang dikirim pelaku, Pesan yang dikirim secara verbal oleh pelaku mengandung cyberbullying sehingga membuat korban merasa di intimidasi oleh pelaku, korban yang merasa di ancam dan di intimidasi kemudian melaporkan pelaku ke pihak kepolisian atas tindakan ancaman verbal melalui media sosial, Setelah pelaku mengirim pesan *Cyberbullying* secara verbal bernada ancaman kepada korban, Pelaku merasa tidak bersalah atas tindakannya, Kemudian kepolisian menyelidiki pelaku di tempat kejadian perkara (TKP) dan ditemukan barang bukti fisik berupa *Smartphone Oppo A37f* dalam keadaan hidup, Pihak kepolisian menyerahkan barang bukti ke laboratorium investigator digital forensik, Investigator melakukan analisa terhadap barang bukti fisik *Smartphone* dan melakukan analisa barang bukti digital yang ditemukan pada *Smartphone*, Setelah di dapatkan pada proses analisa investigator membuat laporan dan menyerahkan barang bukti fisik smartphone dan menyerahkan barang bukti digital pada kepolisian.

II. METODE

Adapun tahapan yang akan di lalui dalam melakukan investigasi bukti digital aplikasi wechat pada smartphone yaitu menggunakan framework Integrated Digital Forensik Proses Model Berbasis SNI 27037:2014 sebagai berikut :



Gambar 2. Framework IDFPM [3]

III. PEMBAHASAN

Pada penelitian ini mempersiapkan seluruh aspek kebutuhan alat dan bahan untuk kepentingan analisis barang bukti digital Aplikasi *WeChat* pada *Smartphone* yaitu *Adb (Android Debug Bridge* untuk komunikasi pada smartphone, *Mobikin assistant for android* untuk mentransfer data , *Usb write blocker* untuk mendeteksi penulisan pada perangkat, *KingRoot* hak akses pada smartphone, *BusyBox* untuk mendapatkan hak akses fitur root, *Autopsy* untuk mencari sumber data, *Mobile edit forensik express* untuk mendekripsi aplikasi wechat, yang dilakukan oleh investigator dalam pencarian bukti digital.

3.1. *Integrated Digital Forensics Process Model (IDFPM)*

Dalam menangani kasus *cyberbullying* aplikasi *wechat* pada *smartphone*, investigator menerapkan prosedur penanganan *integrated digital process model (IDFPM)* untuk menyelesaikan kasus *cyberbullying.* Secara umum tahapan penanganan barang bukti memiliki lima tahapan utama yaitu, *preparation*, *incident*, *incident response*, *digital forensic investigation*, dan *presentation.* Tahapan yang digunakan pada investigasi *smartphone* dapat dilihat pada tahapan berikut ini :

3.1.1. *Preparation*

Merupakan tahapan persiapan yang harus dilakukan pihak kepolisian dalam investigasi penanganan barang bukti.

3.1.2. *Incident*

Merupakan tahapan tim penyidik menganalisis jenis insiden atau kasus sebelum menuju ke tempat kejadian peristiwa, berikut tahapan yang akan dilakukan tim penyidik.

3.1.3. *Incident Response*

Merupakan kegiatan pengamanan yang dilakukan tim penyidik di tempat kejadian peristiwa, berikut ini adalah salah satu bagian penting yang terdapat dalam tahapan *incident response* :

a) *a). Device on or off*

Adalah tahap tim digital forensik menganalisis barang bukti elektronik berupa *smartphone* yang ditemukan dalam kondisi hidup dan dalam keadaan baik atau tidak rusak.

Gambar 3. *Smartphone* yang ditemukan dalam kondisi hidup di TKP

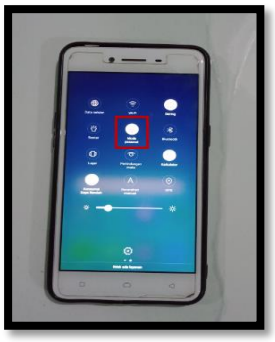
b). Seize

Tahap dimana tim digital forensik memasukkan barang bukti elektronik berupa *smartphone android* di tempat kejadian peristiwa ke kantong barang bukti yang telah di berikan label 01, dapat dilihat pada gambar berikut :

Gambar 4. Pelebelan barang bukti di TKP

b) *c). Preserve*

adalah kegiatan yang dilakukan tim digital forensik untuk melakukan pengamanan, mengisolasi barang bukti elektronik berupa *smartphone android* untuk dilakukan pemindahan barang bukti hingga ke laboraturium digital forensik, sebelum nya dilakukan *airplane mode* agar tidak terkoneksi dengan jaringan dan untuk menjaga integritas data pada barang bukti elektronik berupa *smartphone* yang di dapat di TKP. dapat dilihat pada gambar berikut :



Gambar 5. *Airplane mode* pada barang bukti

3.1.4. Digital Forensic Investigaton

Tahapan yang dilakukan tim digital forensik di laboraturium digital forensik, adapun salah satu bagian penting dalam tahapan ini yaitu:

a). Analysis Request

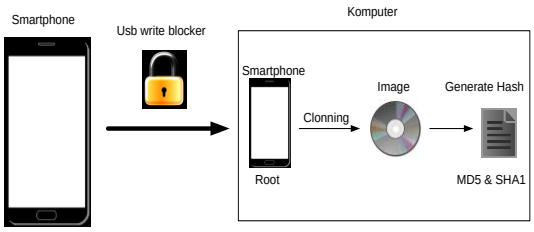
Tahap ini penyidik kepolisian menginginkan pihak investigator untuk mencari barang bukti digital berupa percakapan yang dilakukan secara verbal yang berhubungan dengan barang bukti pelapor.

1. Bukti Pelapor

Gambar 6. Percakapan Melalui Aplikasi *Wechat*

b). Acquisition

Pada tahapan akuisisi diawali dengan menghadirkan satu unit *Smartphone Oppo A37f* milik penulis yang di rekayasa dalam skenario. berikut gambar yang menunjukkan proses akuisisi *Smartphone:*



Gambar 7. Proses Akuisisi *Smartphone* Menggunakan *Framework IDFPM*

2) *c). Authenticate*

Menjelaskan autentifikasi barang bukti digital dengan format *bbOppo.dd* hasil dari akuisisi yang ditemukan oleh investigator dan dilakukan verifikasi barang bukti untuk melihat hasil perbandingan nilai hashing sebelum dan sesudah di akuisisi, dapat dilihat pada gambar berikut ini :

MD5 Hash	
Computed hash	8c5ea87ef41075d54392b4aa2a7bee67
Report Hash	8c5ea87ef41075d54392b4aa2a7bee67
Verify result	Match
SHA1 Hash	
Computed hash	b20da344f6b8cff42d491d837c5d1f7f91e308f9
Report Hash	b20da344f6b8cff42d491d837c5d1f7f91e308f9
Verify result	Match

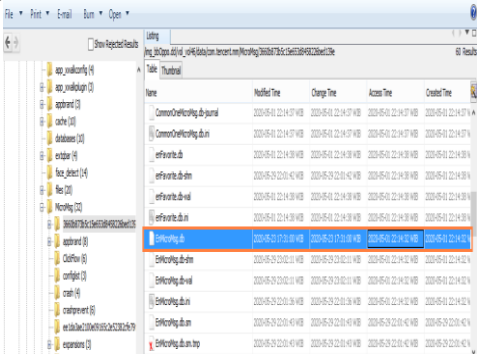
Gambar 8. Nilai *Hashing Sebelum*

```
Image Verification Results:
 Verification started:  Sat May 30 00:50:34 2020
 Verification finished: Sat May 30 00:53:18 2020
 MD5 checksum:    8c5ea87ef41075d54392b4aa2a7bee67 : verified
 SHA1 checksum:   b20da344f6b8cff42d491d837c5d1f7f91e308f9 : verified
```

Gambar 9. Nilai *Hashing* Sesudah Dari *bbOppo.dd*

3) *d). Identify*

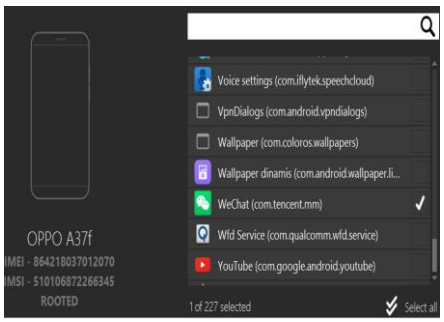
Dalam kegiatan ini investigator mengidentifikasi data yang di dapat dari barang bukti digital hasil akuisisi menggunakan *tools Autopsy*, data tersebut digunakan untuk mencari petunjuk yang berkaitan dengan kasus *cyber-bullying*, serta mencari data yang dapat dicurigai guna mendapatkan petunjuk. Dapat dilihat pada gambar berikut:



Gambar 10. *Database* Yang Dicurigai

e). Analyse

Tahap ini menjelaskan bahwa investigator melakukan analisis barang bukti digital yang telah di curigai secara keseluruhan untuk menemukan petunjuk yang berkaitan dengan adanya kasus *cyberbullying* yang dilakukan secara verbal pada media *Wechat pada smartphone*, secara *teori file Enmicromsg.db* adalah file database *SQLite* terenkripsi , file ini di enkripsi menggunakan *SQLCipher*, perpanjangan *open source* untuk *database SQLite* yang menyediakan 256-bit AES enkripsi, *key* adalah parameter yang penting untuk mendekripsi file database Enmicromsg.db yang dihasilkan dari nilai hash md5, kombinasi Imei dan nilai UIN, investigator melakukan penyelidikan terhadap barang bukti digital yang terdapat pada *smartphone android* dengan media aplikasi *Wechat* menggunakan *tools Mobile edit forensik express* untuk dapat mendekripsi seluruh *database* aplikasi *Wechat* tersebut sehingga bukti digital berupa percakapan dapat di identifikasi, pada gambar berikut dapat dilihat proses ekstraksi aplikasi *Wechat* pada *smartphone android:*

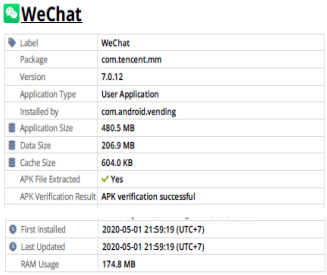


Gambar 11. Pemilihan Aplikasi *Wechat*

Hasil ekstraksi pada *tools mobile edit forensik express* yang dilakukan oleh investigator menjunjukkan bahwa ektraksi di lakukan pada tahun 2020-05-30 yang mana seluruh data terkait bukti digital aplikasi *Wechat* berhasil di dekripsi, gambar berikut ini menunjukkan data hasil ekstraksi aplikasi *wechat* pada *smartphone oppo A37f*:

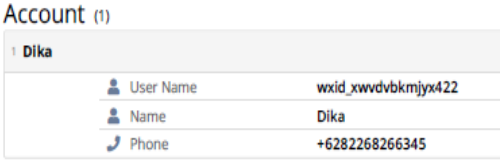
Gambar 12. Hasil Ekstraksi Data Pada *Smartphone*

untuk dapat menganalisis lebih lanjut investigator melakukan pendalaman terhadap bukti digital aplikasi pesan instant *wechat* yang telah ditemukan guna mendapatkan informasi lebih lanjut terkait kasus *cyberbullying* yang dilakukan secara verbal, pada gambar dibawah ini ditemukan spesifikasi dari aplikasi pesan instant *wechat* hasil akuisisi menggunakan *mobileedit forensik express* yang digunakan oleh terduga pelaku:



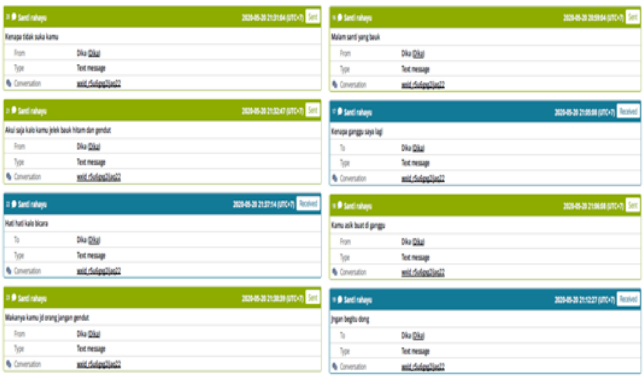
Gambar 13. Spesifikasi Aplikasi *Wechat* Yang Digunakan Terduga Pelaku

pada gambar berikut ini investigator menemukan akun terduga pelaku pengguna aplikasi *wechat* dengan *ID wxid_r5u6gxg2ijaq22*, dengan nama akun dika dan nomor telepon +6282268266345 indonesia , seperti gambar berikut ini:



Gambar 14. Akun Pelaku Yang Ditemukan Pada Aplikasi *Wechat*

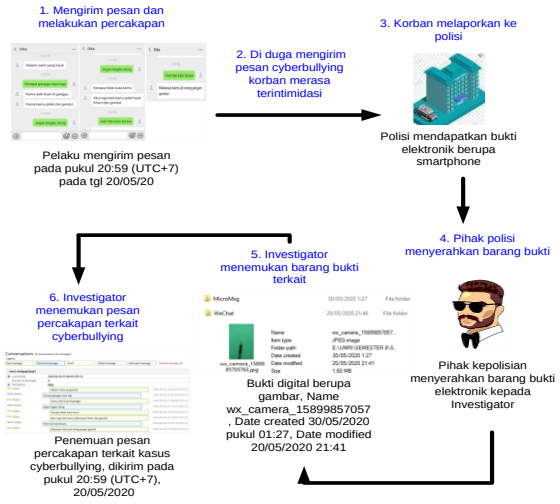
Serta dapat dilihat Timestamp dari percakapan pada gambar di bawah ini pelaku pernah melakukan percakapan dengan isi pesan di awali kalimat “malam santi yang bauk” pada tanggal 20 bulan 05 tahun 2020 pukul 20:59:04 waktu indonesia barat (UTC+7), dapat dilihat pada gambar berikut ini :



Gambar 15. Pesan Percakapan *Cyberbullying* Ditemukan

4) *f). Reconstruct*

Pada tahapan ini investigator melakukan rekonstruksi seluruh barang bukti dari pihak pelapor dan analisa barang bukti yang berkaitan dengan kasus *cyberbullying* secara verbal pada aplikasi *wechat* dengan cara membuat pola dan timestamp :



Gambar 16. Rekonstruksi Pola Dan *TimeStamp*

Berdasarkan gambar diatas menjelaskan bahwa bukti pelapor menunjukkan pelaku mengirim pesan pada pukul 20:59 (UTC+7) pada tanggal 20-05-2020 dan hasil identifikasi percakapan cyberbullying secara verbal yang dilakukan Investigator menunjukkan waktu yang sama bahwa pelaku memang benar pernah melakukan pengiriman pesan cyberbullying secara verbal kepada korban yaitu pukul 20:59 (UTC+7) pada tanggal 20-05-2020, jelas terlihat ada keterkaitannya antara barang bukti pelapor, barang bukti yang ditemukan ditempat kejadian perkara dan barang bukti digital yang telah di analisa Investigator.

3.1.5. *Presentation*

Merupakan kegiatan atau tahapan akhir dari pelaksanaan *digital forensic investigation*, tahap ini investigator melakukan laporan hasil analisis yang di lakukan di laboraturium digital forensik, berupa *chain of custody* dan salinan data terkait kasus *cyberbullying* yang dilakukan secara verbal pada aplikasi *wechat* serta menyimpan salinan barang bukti di laboraturium digital forensik.

IV. SIMPULAN DAN SARAN

Berdasarkan dari hasil penelitian, penerapan *framework Integrated Digital Forensic Process Model* (IDFPM) berbasis SNI 27037:2014 pada proses investigasi *Smartphone Android* dengan media aplikasi *wechat* yang telah dilakukan analisa barang bukti digital bahwa Pesan percakapan Cyberbullying secara verbal pada aplikasi *wechat* berhasil didekripsi. Penerapan *framework Integrated Digital Forensic Process Model* (IDFPM) berbasis SNI 27037:2014 berhasil dilakukan pada proses investigasi forensic dengan media *Smartphone android* sesuai standar operasional prosedur (SOP). Barang bukti berhasil didapatkan dari investigasi forensik pada kasus *cyberbullying* aplikasi media sosial *wechat* berupa pesan percakapan verbal dan nilai *hashing md5* dan *sha1* yang autentik, serta metadata atau *timestamp* pada pesan percakapan aplikasi media sosial *wechat.*

Pada penelitian ini mengenai penerapan *Integrated Digital Forensics Process Model* (IDFPM) berbasis SNI 27037:2014 dan mengenai proses akuisisi aplikasi *wechat* pada proses investigasi *Smartphone*, Terdapat saran untuk pengembangan penelitian selanjutnya yaitu, Melakukan akuisisi lebih spesifik terkait pesan yang telah dihapus pada aplikasi wechat, mengingat bahwa *smartphone* dan aplikasi *wechat* selalu memiliki versi yang lebih tinggi.

REFERENSI

[1] Oktavianti, R. Loisa, R. 2017. "Penggunaan Media Sosial Sesuai Nilai Luhur Budaya di Kalangan Siswa SMA", *Jurnal Pengabdian kepada Masyarakat, Vol. 3, No. 1, ISSN 2460-9447,* https://s3.amazonaws. com/academia.edu.documents/55601 623/PDF _Jurnal_PKM_UGM. Tarumanagara.

[2] Indonesia. Hootsuite Digital, 2019. "*All the data and trends you need to understand internet, social media, mobile and e-commerce behavioursin2019*",https://andi.link/ hootsuite-we-are-social-indonesian-digital-report-2019.

[3] Sudyana, D. Prayudi, Y. Sugiantoro, B. 2019. "*Analysis and evaluation digital forensic investigation framework using iso*" 27037:2012, *International Journal of Cyber-Security and Digital Forensics,* ISSN: 2305-001, https://www.researchgate.net/profile /Didik_Sudyana/publication/328281191_Ana lysis_and_Evaluation_Digital_Forensic_Investigation_ Framework_using_ISO_ 270372012, Pekanbaru.

[4] Unik, M. Larenda, V, G. 2019. "Analisis investigasi android forensic short message service (SMS) pada smartphone", *JOISIE Journal Of Information System And Informatics Engineering*, Vol. 3, No.1, Hlm 10-15, ISSN: 2503-5304, http:// www.ejournal.pelitaindonesia.ac.id/ojs32/i nde x.php/JOISIE /article/view/414 Pekanbaru.

[5] Mohamed, O. Mohamed, K. Hamal, R, B. 2018. "*The uses oh wechat among international students in china, case northeast normaluniversity*", *Educational Technology, School of Information Science and Technology*, E-ISSN No : 2454-9916 | Volume : 4 | Issue : 1, https://oapub.org/edu/index. php/ejae/article/download/1401/4021, China.

[6] Sudyana, D. Putra, R, T. Soni, 2019. "Digital Forensics Investigation on Proxmox Server Virtualization Using SNI 27037:2014", *Journal Publications & Informatics Engineering Research* Volume 3, Number 2, e-ISSN : 2541-2019, *http s:// doi.org/10.33395/sinkron.v3i2.10029,* Pekanbaru.

[7] Mualfah, D. Riadi, I. 2017 "Network Forensics For Detecting Flooding Attack On Web Server", *International Journal of Computer Science and Information Security, Vol.15, No. 2,* ISSN 1947-5500, *https://sites.google.com/site/ijcsis/,* Yogyakarta.

[8] Wu, S. Zhang, Y. Wang, X. Xiong, X. Du, L. 2017. *"Forensic analysis of WeChat on Android smartphones" Proceedings of the 16th Annual USA Digital Forensics Research Conference, www.elsevier.com/locate/diin,* china.

[9] Riadi, I. Yudhana, A. Putra, M, C, F. 2018. "Akuisisi bukti digital pada instagram messenger berbasis android menggunakan metode national institute of justice (NIJ)", *Jurnal Teknik Informatika dan Sistem Informasi,* e-ISSN : 2443-2229 Volume 4 Nomor 2, https://www.resear chgate.net/pr ofile/Imam_Riadi/publication/327779438_Akuisisi_Bukti_Digitl_Pada_InstagramMessenge rBerbasis_Android_Menggu nakan_Metode _National_Institute_Of_Justice_NIJ/, Yog yak arta.

[10] Nasional, Badan Standarisasi. 2014. "SNI 27037:2014 Tentang Teknologi Informasi - Teknik Keamanan - Pedoman