BAB II

LANDASAN TEORI

2.1 *Smartphone*

Smartphone adalah telepon genggam yang mempunyai kemampuan dengan pengunaan dan fungsi yang menyerupai computer, belum ada standar pabrik yang menentukan arti *smartphone*, beberapa orang, *smartphone* merupakan telepon yang bekerja menggunakan seluruh perangkat lunak sistem operasi yang menyediakan hubungan standar dan mendasar bagi pengembang aplikasi. *Smartphone* hanyalah merupakan sebuah telepon yang menyajikan fitur canggih seperti surel (surat elektronik), internet dan kemampuan membaca buku elektronik (*e-book*) atau terdapat papan ketik (baik sebagaimana jadi maupun dihubung keluar), dengan kata lain, *smartphone* merupakan komputer kecil yang mempunyai kemampuan sebuah telepon. Pertumbuhan permintaan akan alat canggih yang mudah dibawa ke mana-mana membuat kemajuan besar dalam pemroses, pengingatan, layar dan sistem operasi yang di luar dari jalur telepon genggam sejak beberapa tahun ini Intan Trivena Maria Daeng, Mewengkang and Kalesaran (2017)**.**

2.2 Cybercrime

Cybercrime adalah aktifitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya.Berdasarkan jenis aktifitas kejahatan yang dilakukan, *cybercrime* dapat digolongkan menjadi beberapa jenis diantaranya adalah pornografi, perjudian *online*, *cyberstalking, cyber-tresspass, dan cyberbullying*.

Semua jeniskejahatan *cyber* tersebut sudah tercantum di dalam undang-undang negara Indonesia. Dasar hukum pidana untuk kejahatan *cyber* di Indonesia, dimuat dalam UU no. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang berisi ketentuan pidana bagi pelaku *cybercrime.* Laporan yang dikeluarkan oleh *RSA Anti Fraud Command Center (AFCC),* menyebutkan bahwa dari tahun 2013 hingga 2015 terjadi peningkatan aktivitas *cybercrime* mencapai 173% di seluruh dunia dengan total kerugian mencapai angka US$ 325 Milyar. Laporan tersebut juga melaporkan bahwa pada tahun 2015 sebesar 45% transaksi dilakukan melalui saluran mobile, sedangkan sebesar 61% penipuan terjadi melalui perangkat mobile (Riadi *et al.*, 2017).

2.3 Digital Forensik

Menurut Mulia Fitriana, Khairan AR (2020) dalam jurnalnya yang berjudul " Penerapan Metode NIST Dalam Analisis Forensik Digital Untuk Penanganan *CyberCrime"*, mendefinisikan Komputer Forensik adalah ilmu yang membahas tentang temuan yang berupa bukti digital setelah peristiwa yang berkaitan dengan keamanan komputer terjadi. Digital Forensik bisa dikatakan penerapan ilmu pengetahuan untuk memulihkan bukti digital dari suatu perangkat baik itu komputer maupun smartphone dengan metode tertentu yang bertujuan untuk mengumpulkan data yang dapat diterima oleh pengadilan sebagai salah satu pembuktian.

2.4 Mobile Forensik

Mobile Forensik merupakan penerapan ilmu pengetahuan untuk memulihkan bukti digital dari perangkat mobile dengan metode yang diterima secara umum

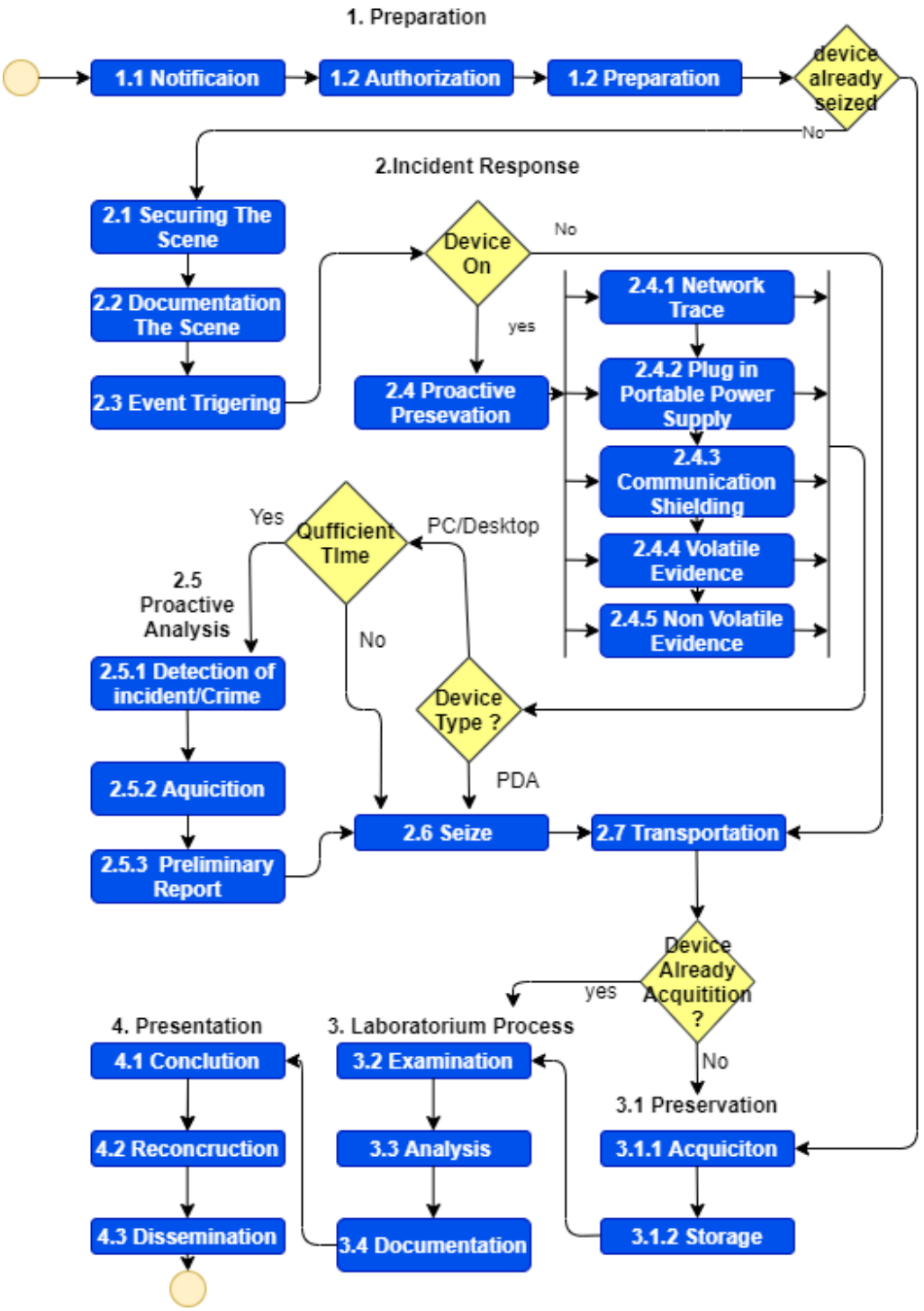
serta memperhatikan aspek legal. Mobile forensics sendiri tidak hanya bertujuan untuk pemenuhan kebutuhan bukti digital di pengadilan (proses litigasi), namun dapat juga digunakan untuk proses non-litigasi. Terlepas dari tujuan akhirnya, seluruh prosedur dan pelaksanaan mobile forensic harus berdasarkan metode umum yang diterima oleh ilmu digital forensics (forensicall sounds) Ridho Firmansyah, M. Akbar no date).

2.5 Whatsapp

WhatsApp merupakan aplikasi perpesanan paling popular saat ini dan merupakan aplikasi perpesanan tak berbayar yang difasilitasi oleh internet. Aplikasi WhatsApp utamanya berjalan pada perangkat seluler, namun juga dapat digunakan pada dekstop selama perangkat seluler yang digunakan terhubung dengan aplikasi WhatsApp pada desktop (Mulia Fitriana, Khairan AR, 2020).

2.6 IDFIF v2

Integrated Digital Forensics Investigation Framework versi 2 (IDFIF v2) merupakan framework terbaru yang telah dikembangkan sehingga diharapkan dapat menjadi standar metode penyelidikan para penyidik karena IDFIF v2 ini memiliki fleksibilitas dalam menangani berbagai jenis barang bukti digital (Ruuhwan, Riadi and Prayudi, 2016). Adapun tahapan-tahapan pada IDFIF v2 ini dapat dilihat pada gambar 1



Gambar 2. 1. Model metode *IDFIF v2*

1) *Preparation*

Persiapan yang harus dilakukan untuk melakukan proses investigasi dalam penanganan barang bukti digital dimulai dari olah tempat kejadian perkara hingga pembuatan laporan akhir.

- *Notification:* Pemberitahuan pelaksanaan investigasi ataupun melaporkan adanya kejahatan kepada penegak hukum.
- *Authorization:* Tahapan untuk mendapatkan hak akses terhadap barang bukti dan status hukum proses penyelidikan.
- *Preparation:* Persiapan yang meliputi ketersediaan alat, personil dan berbagai hal kebutuhan penyelidikan.

2) *Inciden Response*

Kegiatan yang dilakukan di tempat kejadian perkara dengan tujuan untuk mengamankan barang bukti digital yang ada sehingga tidak terkontaminasi oleh hal-hal lain.

- *Securing The Scene:* Melakukan sebuah mekanisme untuk mengamankan TKP dan melindungi integritas barang bukti.
- *Documentation The Scene:* Tujuan pokok dari tahapan ini adalah mengolah tempat kejadian perkara, mencari sumber pemicu kejadian, mencari sambungan komunikasi atau jaringan dan mendokumentasikan tempat kejadian dengan mengambil gambar setiap detail TKP.

- *Event Trigering:* Melakukan analisa awal terhadap sebuah proses kejadian yang terjadi.
- *Proactive Preservation:* Memiliki 5 sub tahapan yaitu *network trace* melakukan pencarian jejak melalui jaringan yang digunakan oleh barang bukti digital. *Plug in portable power supply* merupakan proses pengamanan barang bukti digital dengan kondisi "*on*" sehingga daya yang terdapat pada barang bukti digital tersebut dapat terjaga selama diperjalanan hingga ke laboratorium forensik. *Communication shielding* merupakan tahapan penonaktifan komunikasi data pada barang bukti digital sehingga dapat mencegah perubahan data dari luar. *Volatile dan Non-Volatile evidence* merupakan proses pengamanan barang bukti digital. Di akhir tahap *proactive Preservation* terdapat *decision process*. Tahapan ini memang tidak disebut secara langsung menjadi tahapan, namun *output* dari *decision* ini juga penting untuk keberlangsungan proses penyelidikan. Tahapan ini diputuskan barang bukti digital tersebut harus langsung disita dan dilakukan pemeriksaan lebih lanjut di laboratorium forensik atau dilakukan pemeriksaan di tempat untuk mendapatkan laporan awal kejadian.

- *Proactive Analysis*: tahapan *live analysis* terhadap barang temuan dan membangun hipotesa awal dari sebuah kejadian. *Detection of Incident / Crime*, di tahap ini adalah tahap untuk memastikan bahwa telah terjadi pelanggaran hukum. *Acquicition* merupakan proses akuisisi data terhadap barang temuan sehingga meringankan beban kerja digital forensic analys di laboratorium. *Preliminary Report*, merupakan pembuatan laporan awal atas kegiatan penyelidikan proaktif yang telah dilakukan.
- *Seize:* Melakukan proses penyitaan terhadap barang bukti digital yang telah ditemukan untuk dianalisa lebih lanjut.
- *Transportation:* Merupakan proses pemindahan barang bukti digital dari tempat kejadian perkara menuju laboratorium digital foresik.

3) *Laboratorium Process*

Penanganan barang bukti di tempat kejadian perkara telah selesai, maka pada tahapan ini adalah melakukan proses analisa data terhadap barang bukti yang telah didapatkan sebelumnya sehingga dapat ditemukan jenis kejahatan yang telah terjadi.

- *Preservation:* Menjaga integritas temuan dengan menggunakan *chain of custody* dan fungsi *hashing*.
- *Examinitation:* Pengolahan barang bukti untuk menemukan keterkaitanya dengan kejadian.

- *Analysis:* Merupakan kajian teknis dan merangkai keterkaitan antara temuan-temuan yang ada.
- *Documentation:* melakukan dokumentasi terhadap seluruh kegiatan yang telah dilakukan dari awal proses penyelidikan hingga akhir proses analisa di laboratorium forensik.

4) *Presentation*

Presentation merupakan tahapan akhir dalam proses investigasi digital. Tahapan ini merupakan proses pembuatan laporan terkait hasil analisa yang dilakukan pada tahap sebelumnya dan memastikan bahwa setiap proses yang dilakukan tersebut telah sesuai dengan aturan hukum yang berlaku.

- *Conclution:* Menyimpulkan hasil dari investigasi yang telah dilakukan.
- *Recontruction:* Proses analisa dan evaluasi keseluruhan terhadap hasil investigasi.
- *Dissemination:* Pencatatan proses penyelidikan dan catatan tersebut dapat disebarluaskan pada penyelidik lain yang melakukan penyedikan pada kasus serupa.

2.7 Mobiledit Forensic

MOBILedit merupakan *tool* forensik yang memungkinkan penyidik untuk memperoleh secara logik, mencari dan memeriksa perangkat ponsel. *Tool* ini menggunakan beberapa mekanisme konektivitas terutama konektivitas

nirkabel dibandingkan tool sejenis. *Software* ini cukup baik digunakan untuk memperoleh informasi sistem telepon dan informasi lainnya seperti daftar kontak dan pesan.

2.8 Magnet AXIOM

Magnet AXIOM merupakan *platform* yang menangkap dan menganalisis *smartphone,* komputer, *cloud,* IoT, dan hasil *imaging* dari *software* lain. *Axiom* menyederhanakan invetigasi dengan menampilkan barang bukti yang relevan sebagai artefak yang mudah untuk dilihat.

2.9 Penelitian Terkait

Tabel 2. 1 Penelitian Terkait

No	Peneliti	Metode dan *Tools*	Judul Penelitian	Hasil Penelitian
1	Muhammad Irwan Syahib, Imam Riadi, Rusydi Umar (2018)	*National Institute of Standard Technology (NIST)* dan *tools* Oxygen Forensic, MobilEdit Forensic	Analisis Forensik Digital Aplikasi *Beetalk* untuk Penaganan *Cybercrime* menggunakan metode NIST	Mengetahui barang bukti digital pada kasus *Cybercrime*
2	Riski Yudhi Prasongko, Anton Yudhana, Abdul Fadil (2018)	*National Institute of Standard Technology (NIST)* dan *tools MobilEdit Forensic*	Analisa Forensik Aplikasi *Kakaotalk* menggunakan Metode *National Institute of Standard Technology (NIST)*	Mengetahui barang bukti digital pada kasus *Cybercrime*
3	Mulia Fitriana, Khairan AR, Jiwa Malem Marsya (2020)	*National Institute of Standard Technology (NIST)* dan *tools FTK Imager*	Penerapan Metode *National Institute of Standard Technology (NIST)* dalam analysis forensic digital untuk penaganan *Cybercrime*	Mengetahui barang bukti digital pada kasus *Cybercrime*
4	Imam Riadi, Anton Yudhana,Muhamad	*National Institute of Standard*	Analisis *Recovery* bukti digital	Mengetahui barang bukti

	Caesar Febriansyah Putra (2017)	*Technology (NIST)* dan *tools Oxygen Forensic*	*Instagram Messengger* menggunakan metode *National Institute of Standard Technology (NIST)*	digital pada kasus *Cybercrime*
5	Anton Yudhana, Imam Riadi, Ikhwan Anshori (2018)	*National Institute of Standard Technology (NIST)* dan *tools Oxygen Forensic*	Analisi bukti digital *Facebook Messengger* menggunakan metode *NIST*	Mengetahui barang bukti digital pada kasus *Cybercrime*
6	Anton Yudhana, Rusydi Umar, Ahwan Ahmadi (2019)	*National Institute of Standard Technology (NIST)* dan *tools MobilEdit Forensic*	*Digital Evidence Identification on Google Drive in Android Device Using NIST Mobile Forensic Method*	Mengetahui barang bukti digital pada kasus *Cybercrime*
7	Saleh Khalifa Saad, RusydiUmar, Abdul Fadlil (2020)	*National Institute of Standard Technology (NIST)* dan *tools*	Analisis Forensik Aplikasi Dropbox Pada Android Menggunakan Metode *NIST*	membandingkan direktori dan database dibuat dari aktivitas-aktivitas tersebut
8	Mustafa, Imam Riadi, Rusydi Umar (2018)	*National Institute of Standard Technology (NIST)* dan *tools Aid4Mail Forensic*	Rancangan Investigasi Forensik *E-mail* Dengan Metode *National Institute of Standard Technology (NIST*	Mengetahui aktivitas pengiriman *E-mail* palsu
9	Rusydi Umar, Sahiruddin (2019)	*National Institute of Standard Technology (NIST)* dan *tools Wondershare dr. Fone for Android, Oxygen Forensic Suite 2014*	Metode *NIST* Untuk Analisis Forensik Bukti Digital Pada Perangkat Android	Mengetahui barang bukti digital pada kasus *Cybercrime*
10	Gregorius Hendita Artha Kusuma, Yusuf Fadhilah (2019)	*National Institute of Standard Technology (NIST)*	Analisis Forensik Digital *E-Commerce* pada *Website* Rental Mobil Menggunakan Metode *NIST*	Mengetahui bahwa *web* tersebut adalah penipu

11	Doddy Teguh Yuwono, Siti Juhairiah, Sonedi (2019)	*National Institute of Standard Technology (NIST)* dan *tools FTK Imager, Autopsy*	Analisis *File Carving* Pada *File System* Dengan Metode *National Institute of Standard Technology (NIST)*	Mengetahui *File-file* yang telah terhapus
12	Imam Riadi, Abdul Fadlil, Muhammad Nasir Hafizh (2020)	*National Institute of Standard Technology (NIST)* dan *tools Wireshark, Ettercap*	Analisis Bukti Serangan *Address Resolution Protocol Spoofing* menggunakan Metode *National Institute of Standard Technology*	Mengidentifikasi serangan *ARP Spoofing*
13	Muhammad Abdul Aziz Imam Riadi , Rusydi Umar (2018)	*National Institute of Justice (NIJ)* dan *tools FTK Imager*	Analisis Forensik *Line Messengger* berbasis *Web* menggunakan *Framework National Institute of Justice (NIJ)*	Mengetahui barang bukti digital pada kasus *Cybercrime*
14	Anton Yudhana, Abdul Fadlil, Muhammad Rizki Setyawan (2017)	*National Institute of Standard Technology (NIST)* dan *tools Oxygen Forensic Suite 2014, Belkasoft Evidience Center*	Analisis Recovery Bukti Digital Skype berbasis Smartphone Android Menggunakan Framework NIST	Mengembalikan barang bukti digital pada kasus *Cybercrime*
15	Arsyian Aldi Warsito (2020)	*NIST MEASUREMENTS*	Analisis Kinerja *Autopsy* pada *Smartphone* berbasis Android Menggunakan *NIST MEASUREMENTS*	Mengembalikan barang bukti digital pada kasus *Cybercrime*
16	Sidik Madiyanto, Husni Mubarok, Nur Widiyasono (2017)	*IDFIF v2* dan *tools Magnet Axiom*	Proses Investigasi *Mobile Forensik* Pada *Smartphone* Berbasis *IOS*	Mengembalikan barang bukti berupa pesan teks pada kasus *Cybercrime*

Tabel 2.1 adalah hasil *study literature* yang telah dilakukan sebelum penelitian dilakukan. Tabel 2.1 semua menjelaskan tentang bagaimana melakukan

analisis dan investigasi pada kasus *Cybercrime. Study literature* yang telah dilakukan akan membantu dalam penelitian ini.

Tabel 2. 2 Penelitian Terdekat

No	Peneliti	Metode dan *Tools*	Judul Penelitian	Hasil Penelitian
1	Sidik Madiyanto, Husni Mubarok, Nur Widiyasono (2017)	*IDFIF v2* dan *tools Magnet Axiom*	Proses Investigasi *Mobile Forensik* Pada *Smartphone* Berbasis *IOS*	Mengembalikan barang bukti berupa pesan teks *SMS* pada kasus *Cybercrime*
2	Ruuhwan , Imam Riadi, Yudi Prayudi (2016)	*IDFIF v2* dan *tools MobilEdit Forensic*	Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) pada Proses Investigasi Smartphone	Mengembalikan barang bukti digital pada kasus *Cybercrime* berupa Riwayat panggilan dan pesan teks *SMS*
3	Usulan penelitian yang akan dilakukan oleh Muhammad Faisal Hikam Nur Widyasono (2020)	*IDFIF v2* dan *tools MOBILedit forensic* dan *Magnet AXIOM*	Analsisi dan Investigasi *Cybercrime* Pada *Smartphone* Berbasis android menggunakan metode IDFIF v2	Mengembalikan barang bukti pada aplikasi *Whatsapp* berupa gambar, video, dan pesan teks.

Tabel 2.2 adalah penelitian yang telah dilakukan sebelumnya mengenai proses investigasi *Cybercrime.* Penelitian yang berjudul "Proses Investigasi *Mobile Forensik* Pada *Smartphone* Berbasis *IOS"* dengan penulis (Madiyanto, Mubarok and Widiyasono, 2017). Tahapan yang dilakukan adalah menggunakan metode *Integrated Digital Forensics Investigation Framework versi 2 (IDFIF v2)* dan dibantu dengan *tools Magnet Axiom* sehingga mampu mengungkap kejahatan yang terjadi pada *Smartphone IOS* dengan mencari barang bukti digital berupa pesan teks yang telah dihapus.

Penelitian yang berjudul "Analisis Forensik Digital Aplikasi *Beetalk* untuk Penaganan *Cybercrime* menggunakan metode NIST" oleh (Syahib, Riadi and Umar, 2018) dimana peneliti melakukan analisi dan proses invetigasi terhadap *Cybercrime* pada aplikasi *Instant Message Beetalk* dengan menggunakan metode *National Institute of Standard Technology (NIST)* dan dibantu dengan *tools Oxygen Forensics* dan *MobilEdit Forensic* dengan mengungkap barang bukti digital berupa gambar dan pesan teks.

Penelitian yang telah di lakukan di atas telah memenuhi aspek yang dibutuhkan untuk penelitian yang akan di lakukan yang berjudul " "

2.10 Matriks Penelitian

Tabel 2. 3 Matriks Penelitian

No	Judul	Peneliti	Tahun	Ruang Lingkup								Keterangan
				Metode		Sistem Operasi			Tools Forensic			
				NIST	NIJ	Android	IOS	windows	Oxygen Forensic	Mobil Edite Forensic	Ftk Imager	
1	ANALISIS FORENSIK DIGITAL APLIKASI BEETALK UNTUK PENANGANAN	Muhammad Irwan Syahib, Imam	24 November 2018	✓		✓			✓	✓		Barang bukti digital (Gambar dan teks)

	CYBERCRIME MENGGUNAKAN METODE NIST	Riadi, Rusydi Umar										
2	ANALISA FORENSIK APLIKASI KAKAOTALK MENGGUNAKAN METODE NATIONAL INSTITUTE STANDARD TECHNOLOGY	Riski Yudhi Prasongko, Anton Yudhana, Abdul Fadil	24 November 2018	✓		✓				✓		Barang bukti digital (Gambar dan teks)
3	PENERAPAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) DALAM ANALISIS FORENSIK DIGITAL UNTUK PENANGANAN CYBER CRIME	Mulia Fitriana, Khairan AR, Jiwa Malem Marsya	Maret 2020	✓		✓					✓	Barang bukti digital (teks)
4	ANALISIS RECOVERY BUKTI DIGITAL INSTAGRAM MESSANGERS MENGGUNAKAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)	Imam Riadi, Anton Yudhana,Muhamad Caesar Febriansyah Putra	2017	✓		✓						Barang bukti digital (Gambar dan teks)
5	Analisis Bukti Digital Facebook Messenger	Anton Yudhana, Imam	Agustus 2018	✓		✓			✓			Barang bukti digital (akun,

	Menggunakan Metode Nist	Riadi, Ikhwan Anshori										gambar, teks, audio, video)
6	Digital Evidence Identification on Google Drive in Android Device Using NIST Mobile Forensic Method	Anton Yudhana, Rusydi Umar, Ahwan Ahmadi	Mei 2019	✓		✓				✓		Bukti digital (gambar, video,zip, rar, pdf, docx, ppttx, app, data base)
7	Analisis Forensik Aplikasi Dropbox Pada Android Menggunakan Metode NIS	Saleh Khalifa Saad, RusydiUmar, Abdul Fadlil		✓		✓						Data
8	RANCANGAN INVESTIGASI FORENSIK EMAIL DENGAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)	Mustafa, Imam Riadi, Rusydi Umar	2018	✓				✓				Bukti digital data
9	METODE NIST UNTUK ANALISIS FORENSIK BUKTI DIGITAL PADA PERANGKAT ANDROID	Rusydi Umar, Sahiruddin	2019	✓		✓			✓			Barang bukti digital (kontak, log panggilan, pesan)
10	Analisis Forensik Digital E-Commerce pada Website Rental Mobil	Gregorius Hendita Artha	2019	✓				✓				Barang bukti bahwa web tersebut

	Menggunakan Metode NIST	Kusuma, Yusuf Fadhilah										melakukan penipuan
11	ANALISIS FILE CARVING PADA FILE SYSTEM DENGAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)	Doddy Teguh Yuwono, Siti Juhairiah, Sonedi	November 2019	✓				✓			✓	Reporting file yang dihapus, disembunyikan, dan diformat
12	Analisis Bukti Serangan Address Resolution Protocol Spoofing menggunakan Metode National Institute of Standard Technology	Imam Riadi, Abdul Fadlil, Muhammad Nasir Hafizh	6 Mei 2020	✓				✓				Laporan bukti serangan (sumber, korban, waktu)
13	ANALISIS FORENSIK LINE MESSENGER BERBASIS WEB MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF JUSTICE (NIJ)	Muhammad Abdul Aziz , Imam Riadi , Rusydi Umar	24 November 2018		✓			✓			✓	Barang bukti digital (gambar)
14	Analisis Recovery Bukti Digital Skype berbasis Smartphone Android Menggunakan Framework NIS	Anton Yudhana, Abdul Fadlil, Muhammad Rizki Setyawan	Agustus 2020	✓		✓			✓			Barang bukti digital (gambar, pesan, kontak).

15	ANALISIS KINERJA AUTOPSY PADA SMARTPHONE BERBASIS ANDROID MENGGUNAKAN NIST MEASUREMENTS	ARSYIAN ALDI WARSITO	2020	✓		✓					✓	Barang bukti digital berupa percakapan.
16	PROSES INVESTIGASI MOBILE FORENSIK PADA SMARTPHONE BERBASIS IOS	Sidik Madiyanto, Husni Mubarok, Nur Widiyasono	1 juni 2017	*IDFIF v2*			✓		Magnet Axiom			Barang bukti digital (pesan teks)