Journal of Applied Informatics and Computing (JAIC)
Vol.x, No.x, Juli 201x, pp. xx~xx
e-ISSN: 2548-6861

Analisis Tingkat Kesadaran Forensik Digital Pada Mahasiswa Rekayasa Keamanan Siber Di Politeknik Negeri Batam

Fahri Wal Fahruddin[1*], Festy Winda Sari[2]**
Program Studi Rekayasa Keamanan Siber (RKS), Politeknik Negeri Batam
Jl. Ahmad Yani, Batam Centre, Batam 29461, Indonesia
fahriwalfahruddin09@gmail.com [1], festy@polibatam.ac.id [2]

Article history:

Received …
Revised …
Accepted …

Keyword:
Forensik Digital, ISO/IEC 27037, Kesadaran, Knowledge Attitude Behavior (KAB).

ABSTRAK

Forensik digital berperan penting dalam mengungkap kronologi, sumber, dan dampak insiden keamanan siber secara sistematis, namun keberhasilan investigasi tersebut sangat bergantung pada kesadaran individu yang menangani bukti digital, bukan semata-mata pada prosedur teknis. Penelitian ini menganalisis tingkat kesadaran forensik digital pada mahasiswa Program Studi Rekayasa Keamanan Siber (RKS) Politeknik Negeri Batam dengan mengintegrasikan pendekatan Knowledge, Attitude, and Behavior (KAB) dan empat tahapan ISO/IEC 27037, yaitu Identification, Collection, Acquisition, dan Preservation. Penelitian ini menggunakan pendekatan kuantitatif, dengan data dikumpulkan dari 68 mahasiswa aktif melalui kuesioner daring sebanyak 24 butir pernyataan yang dipilih menggunakan purposive sampling. Instrumen diuji validitasnya menggunakan korelasi Pearson Product Moment dan diuji reliabilitasnya menggunakan Alpha Cronbach, yang keduanya menunjukkan bahwa seluruh butir valid dan sangat reliabel 0,934. Analisis deskriptif menunjukkan bahwa skor rata-rata kesadaran forensik digital secara keseluruhan sebesar 3,629, tergolong kategori sangat tinggi. Pada tingkat indikator, Collection memperoleh skor tertinggi 3,647, diikuti Preservation 3,645, Identification 3,640, dan Acquisition 3,583 sebagai skor relatif terendah. Pada tingkat dimensi, Attitude memperoleh skor tertinggi 3,746, diikuti Behavior 3,610 dan Knowledge 3,529. Temuan ini menunjukkan bahwa mahasiswa RKS telah memahami, menilai penting, dan menerapkan penanganan bukti digital sesuai ISO/IEC 27037, meskipun pengetahuan teoretis, khususnya pada tahapan Acquisition, masih memerlukan penguatan dalam kurikulum program studi.

I. PENDAHULUAN

Perkembangan teknologi informasi yang pesat turut meningkatkan ancaman keamanan siber di berbagai sektor kehidupan. Badan Siber dan Sandi Negara mencatat sekitar 5,2 miliar anomali trafik internet yang berpotensi menjadi serangan siber sepanjang tahun 2025, dan sebagian besar anomali tersebut berkaitan dengan malware yang dapat berkembang menjadi ransomware [1]. Berbagai teknologi pencegahan telah dikembangkan, namun insiden tetap dapat terjadi bukan karena kegagalan teknis sistem, melainkan karena faktor human error dari pengguna digital [2]. Untuk itu, setiap insiden perlu diinvestigasi melalui proses forensik digital guna mengungkap kronologi, sumber, dan dampak insiden secara sistematis dan dapat dipertanggungjawabkan.

Kompleksitas insiden keamanan siber turut meningkatkan pentingnya bukti digital sebagai unsur utama dalam proses investigasi, baik untuk kepentingan teknis maupun hukum. Bukti digital berbeda dengan bukti fisik konvensional karena sifatnya yang mudah berubah (volatile) dan rentan terhadap kontaminasi maupun kerusakan apabila tidak ditangani dengan prosedur yang tepat sejak tahap paling awal. Kesalahan sekecil apa pun pada tahap identifikasi atau pengumpulan dapat menimbulkan efek berantai yang menurunkan nilai pembuktian bukti digital pada tahap analisis maupun pelaporan, sehingga kesadaran individu yang menangani bukti sejak awal proses menjadi penentu keberhasilan investigasi secara keseluruhan.

Forensik digital merupakan proses identifikasi, pengumpulan, analisis, dan pelaporan bukti digital yang harus dilakukan secara sistematis agar dapat dipertanggungjawabkan secara hukum maupun teknis. Penerapan standar baku, seperti ISO/IEC 27037, terbukti berperan penting dalam menjaga keterlacakan, dokumentasi, dan keabsahan bukti digital [3]. Pemahaman terhadap pentingnya standar tersebut perlu dibekalkan sejak masa pendidikan, khususnya bagi mahasiswa yang kelak berperan sebagai tenaga ahli di bidang keamanan dan forensik digital, mengingat tingkat kesadaran keamanan siber di kalangan mahasiswa secara umum masih tergolong rendah [4].

Rendahnya kesadaran tersebut dapat dipahami melalui pendekatan Knowledge, Attitude, and Behaviour (KAB), yang menjelaskan bahwa kesadaran seseorang terhadap suatu

praktik keamanan terbentuk dari keterkaitan antara pengetahuan, sikap, dan perilaku nyata dalam penerapannya [5]. Dalam kerangka ini, seseorang dapat memiliki pengetahuan yang memadai, tetapi belum tentu menunjukkan sikap dan perilaku yang konsisten dalam praktiknya, sebagaimana ditemukan pada mahasiswa yang cenderung memiliki pengetahuan keamanan informasi memadai namun belum diimbangi sikap dan perilaku yang konsisten [6].

Mahasiswa Program Studi Rekayasa Keamanan Siber (RKS) Politeknik Negeri Batam merupakan pihak yang relevan untuk dikaji, mengingat kurikulumnya telah mencakup mata kuliah Forensik Siber [7]. Namun, penelitian mengenai kesadaran mahasiswa selama ini umumnya membahas keamanan siber atau data pribadi secara umum, tanpa dikaitkan secara spesifik dengan tahapan forensik digital, sekalipun pada mahasiswa dengan latar belakang teknis [8]. Berdasarkan uraian tersebut, penelitian ini bertujuan menganalisis tingkat kesadaran forensik digital pada mahasiswa RKS Politeknik Negeri Batam dengan mengintegrasikan pendekatan KAB dan empat tahapan indikator ISO/IEC 27037, sehingga dapat menjadi dasar evaluasi dan pengembangan kurikulum yang lebih relevan dengan kebutuhan kompetensi di bidang keamanan dan forensik digital.

Penelitian oleh Tan et al. [4] misalnya berfokus pada kesadaran keamanan siber mahasiswa lintas program studi di Kota Batam tanpa menyentuh tahapan spesifik forensik digital, sementara Arum et al. [6] menyoroti kesenjangan antara sikap dan pengetahuan keamanan informasi menggunakan instrumen HAIS-Q yang bersifat umum dan tidak spesifik pada konteks bukti digital. Demikian pula, Parhusip et al. [8] membandingkan kesadaran keamanan data pribadi antara mahasiswa Teknik Informatika dan non-Teknik Informatika, namun belum mengaitkan temuannya dengan kerangka penanganan bukti digital seperti ISO/IEC 27037. Ketiga penelitian tersebut memberikan gambaran umum kesadaran keamanan siber atau data pribadi, tetapi belum memetakan kesadaran secara spesifik pada tahapan teknis penanganan bukti digital, sehingga belum dapat digunakan secara langsung untuk mengevaluasi kesiapan mahasiswa program studi keamanan siber dalam praktik forensik digital.

Kebaruan penelitian ini terletak pada penggabungan dua kerangka analisis, yaitu pendekatan Knowledge, Attitude, and Behavior (KAB) dan empat tahapan ISO/IEC 27037, yang diterapkan secara spesifik pada mahasiswa program studi keamanan siber, berbeda dengan penelitian terdahulu yang umumnya mengukur kesadaran keamanan siber atau data pribadi secara umum tanpa mengaitkannya dengan tahapan penanganan bukti digital.

Secara teoretis, penelitian ini diharapkan memperkaya kajian mengenai kesadaran keamanan siber dengan menawarkan kerangka pengukuran yang lebih rinci dan spesifik pada konteks penanganan bukti digital, sehingga dapat menjadi rujukan bagi penelitian sejenis pada program studi keamanan siber lainnya. Secara praktis, hasil penelitian ini diharapkan dapat memberikan masukan bagi pengelola Program Studi RKS Politeknik Negeri Batam dalam mengevaluasi capaian pembelajaran mata kuliah Forensik Siber, khususnya dalam menentukan prioritas penguatan materi maupun praktikum pada tahapan yang teridentifikasi masih relatif lemah.

II. METODE

A. Landasan Teori

Kesadaran adalah kondisi seseorang memahami dan menyadari pentingnya suatu hal sehingga terdorong bertindak dengan tepat. Model Knowledge-Attitude-Behavior (KAB) yang dikembangkan oleh Kruger & Kearney [5] menjelaskan kesadaran melalui tiga dimensi, yaitu Knowledge (sejauh mana seseorang memahami suatu topik), Attitude (pandangan atau penilaian terhadap pentingnya suatu hal), dan Behavior (tindakan nyata yang dilakukan seseorang). Sikap keamanan siber yang positif terbukti berperan penting dalam membentuk kesadaran mahasiswa di era digital, sebagaimana ditemukan pada mahasiswa perguruan tinggi.

Forensik digital adalah proses identifikasi, pengumpulan, dan analisis bukti digital yang digunakan untuk mengungkap penyebab suatu insiden keamanan siber [3]. Proses ini harus dilakukan secara hati-hati karena bukti digital mudah berubah atau rusak apabila tidak ditangani dengan prosedur yang benar. Standar ISO/IEC 27037 mengatur pedoman penanganan bukti digital yang mencakup empat tahapan, yaitu Identification (mengenali sumber bukti), Collection (mengumpulkan bukti fisik sesuai prosedur), Acquisition (menyalin data melalui proses imaging tanpa merusak data asli), dan Preservation (menjaga bukti digital agar tetap utuh) [3]. Standar ini telah banyak diterapkan pada berbagai kasus, misalnya pada forensik rekaman CCTV dan investigasi bukti digital pada kasus penipuan e-commerce, sehingga relevan dijadikan acuan untuk mengukur kesadaran mahasiswa secara menyeluruh.

Kesadaran forensik digital dapat dipahami sebagai pertemuan antara dimensi kesadaran (Knowledge, Attitude, Behavior) dan tahapan penanganan bukti digital menurut ISO/IEC 27037. Semakin tinggi kesadaran seseorang pada ketiga dimensi tersebut, semakin besar peluang bukti digital ditangani sesuai prosedur yang benar sehingga integritas dan keaslian bukti tetap terjaga.

Secara operasional, kombinasi antara dimensi KAB dan tahapan ISO/IEC 27037 dalam penelitian ini dapat diuraikan sebagai berikut. Pada tahap Identification, Knowledge merujuk pada pemahaman mahasiswa mengenai jenis-jenis sumber bukti digital, Attitude merujuk pada penilaian pentingnya identifikasi yang tepat sejak awal penanganan insiden, dan Behavior merujuk pada kebiasaan memeriksa perangkat secara sistematis sebelum bukti dipindahkan. Pada tahap Collection, ketiga dimensi tersebut berkaitan dengan pemahaman prosedur pengumpulan barang bukti fisik, kesediaan mengikuti prosedur rantai penyimpanan (chain of

custody), dan praktik pendokumentasian proses pengumpulan secara konsisten. Pada tahap Acquisition, dimensi tersebut mencakup pemahaman teknis mengenai proses imaging dan verifikasi hash, kesadaran akan pentingnya menjaga integritas data asli selama proses penyalinan, serta praktik penggunaan write blocker atau perangkat forensik yang sesuai standar. Pada tahap Preservation, ketiganya berkaitan dengan pemahaman metode penyimpanan bukti digital jangka panjang, penilaian terhadap risiko kerusakan atau kehilangan bukti, dan kebiasaan mendokumentasikan rantai penyimpanan bukti secara konsisten hingga proses investigasi selesai. Uraian operasional inilah yang menjadi dasar penyusunan 24 butir pernyataan sebagaimana disajikan pada Tabel I.

B. Jenis Penelitian

Penelitian ini menggunakan metode kuantitatif untuk memperoleh data dalam bentuk angka yang selanjutnya dianalisis secara statistik guna mengetahui tingkat kesadaran forensik digital mahasiswa RKS Politeknik Negeri Batam [8]. Data dikumpulkan menggunakan kuesioner yang disusun berdasarkan empat tahapan ISO/IEC 27037, yaitu Identification, Collection, Acquisition, dan Preservation, yang masing-masing diukur melalui dimensi Knowledge, Attitude, dan Behavior (KAB).

C. Populasi dan Sampel

Populasi penelitian adalah mahasiswa aktif Program Studi RKS Politeknik Negeri Batam tahun akademik 2025/2026 yang telah menempuh mata kuliah forensik digital sesuai struktur kurikulum program studi [7]. Sampel ditentukan menggunakan teknik purposive sampling dengan kriteria: (1) mahasiswa aktif Program Studi RKS Politeknik Negeri Batam tahun akademik 2025/2026, dan (2) bersedia menjadi responden secara sukarela. Kuesioner disebarkan secara daring dan diperoleh 68 responden yang memenuhi kriteria tersebut.

Pemilihan teknik purposive sampling didasarkan pada pertimbangan bahwa kesadaran forensik digital hanya relevan diukur pada mahasiswa yang telah atau sedang memperoleh paparan materi terkait, sehingga mahasiswa yang tidak memenuhi kriteria tersebut dikeluarkan dari populasi sasaran. Jumlah 68 responden yang diperoleh merepresentasikan sebagian besar populasi mahasiswa aktif Program Studi RKS pada rentang semester yang telah maupun sedang menempuh mata kuliah forensik digital, sehingga data yang terkumpul dapat dianggap cukup representatif untuk menggambarkan kesadaran forensik digital pada populasi tersebut, meskipun generalisasi ke luar konteks program studi maupun institusi perlu dilakukan secara hati-hati.

D. Instrumen dan Skala Pengukuran

Instrumen penelitian berupa kuesioner tertutup dengan 24 butir pernyataan yang mencakup empat indikator ISO/IEC 27037 dan tiga dimensi KAB, dengan masing-masing kombinasi indikator-dimensi diwakili oleh dua butir pernyataan, sebagaimana disajikan pada Tabel I. Setiap butir diukur menggunakan Skala Likert 4 poin, dengan skor 4 untuk Sangat Setuju, 3 untuk Setuju, 2 untuk Tidak Setuju, dan 1 untuk Sangat Tidak Setuju.

Penyusunan butir pernyataan mengacu pada definisi operasional tiap kombinasi indikator-dimensi yang telah diuraikan pada bagian Landasan Teori, kemudian disesuaikan bahasanya agar mudah dipahami oleh mahasiswa tanpa mengubah substansi konsep yang diukur. Sebelum disebarkan, instrumen terlebih dahulu ditinjau secara konseptual untuk memastikan setiap butir hanya mengukur satu aspek dan tidak tumpang tindih antar indikator maupun antar dimensi, sehingga hasil pengukuran dapat dipahami secara tepat baik pada tingkat butir, indikator, maupun dimensi.

TABEL I KISI-KISI INSTRUMEN PENELITIAN

Indikator	Knowledge	Attitude	Behavior	Total
Identification	2	2	2	6
Collection	2	2	2	6
Acquisition	2	2	2	6
Preservation	2	2	2	6
Total Butir	**8**	**8**	**8**	**24**

Ringkasan skor pada setiap pilihan jawaban Skala Likert 4 poin yang digunakan dalam kuesioner disajikan pada Tabel II.

TABEL II SKALA PENILAIAN LIKERT

Skor	Kategori Jawaban
4	Sangat Setuju
3	Setuju
2	Tidak Setuju
1	Sangat Tidak Setuju

Keterkaitan antar variabel penelitian, yaitu dimensi KAB dan indikator ISO/IEC 27037 sebagaimana diuraikan pada bagian Landasan Teori, digambarkan melalui model konseptual penelitian pada Gambar 1 berikut.

Gambar 1. Model Konseptual Penelitian

E. Teknik Analisis Data

Data yang terkumpul dianalisis melalui tiga tahap, yaitu uji validitas, uji reliabilitas, dan analisis deskriptif [4]. Uji validitas menggunakan teknik korelasi Pearson Product Moment (1), dengan membandingkan nilai r hitung tiap butir terhadap nilai r tabel pada taraf signifikansi α = 0,05 dan derajat bebas df = n − 2. Butir dinyatakan valid apabila r hitung > r tabel.

$$r_{xy} = \frac{n\sum XY - (\sum X)(\sum Y)}{\sqrt{[n\sum X^2 - (\sum X)^2][n\sum Y^2 - (\sum Y)^2]}}$$

Keterangan:

rxy = koefisien korelasi antara skor butir (X) dan skor total (Y).
n = jumlah responden.
X = skor butir pernyataan yang diuji.
Y = skor total seluruh butir.
ΣXY = jumlah hasil kali skor X dan Y.
ΣX, ΣY = jumlah skor X dan jumlah skor Y.
ΣX^2, ΣY^2 = jumlah kuadrat skor X dan jumlah kuadrat skor Y.

Uji reliabilitas menggunakan koefisien Alpha Cronbach (2), dengan instrumen dinyatakan reliabel apabila nilai koefisien ≥ 0,70 [4].

$$r_{11} = \left(\frac{k}{k-1}\right)\left(1 - \frac{\sum \sigma_i^2}{\sigma_t^2}\right)$$

Keterangan:

α = koefisien reliabilitas Alpha Cronbach.
k = jumlah butir pernyataan.
$\Sigma\sigma_i^2$ = jumlah varians skor tiap butir.
σ_t^2 = varians skor total.

Analisis deskriptif dilakukan dengan menghitung skor rata-rata jawaban responden (3), yang selanjutnya dikategorikan ke dalam empat tingkatan kesadaran sebagaimana Tabel III.

Skor rata-rata dihitung secara berjenjang, yaitu dimulai dari skor tiap butir untuk masing-masing responden, kemudian skor rata-rata tiap indikator dan dimensi dari kombinasi butir yang terkait, hingga skor rata-rata keseluruhan sebagai representasi umum tingkat kesadaran forensik digital. Pendekatan berjenjang ini memungkinkan analisis dilakukan tidak hanya pada tingkat agregat, tetapi juga pada tingkat indikator, dimensi, dan bahkan butir individual, sehingga bagian yang relatif lebih lemah dapat diidentifikasi secara lebih presisi.

$$\bar{X} = \frac{\sum_{i=1}^{n} X_i}{n}$$

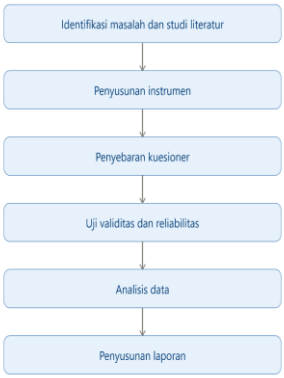
Keterangan:

$\bar{x}$ = skor rata-rata.
Σx = jumlah skor jawaban responden pada butir/kelompok butir yang dihitung.
n = jumlah data yang dirata-ratakan (jumlah butir untuk skor rata-rata tiap responden, atau jumlah responden untuk skor rata-rata tiap butir/indikator/dimensi).

TABEL III KATEGORI TINGKAT KESADARAN

Rentang Skor Rata-rata	Kategori
1,00 – 1,75	Sangat Rendah
1,76 – 2,50	Rendah
2,51 – 3,25	Tinggi
3,26 – 4,00	Sangat Tinggi

Tahapan pelaksanaan penelitian, mulai dari perumusan masalah hingga penarikan kesimpulan, disajikan secara ringkas melalui alur penelitian pada Gambar 2 berikut.

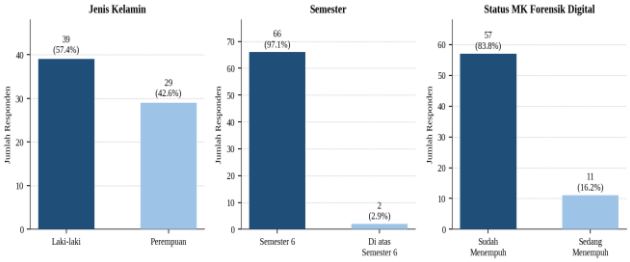


Gambar 2. Alur Penelitian

III. HASIL DAN PEMBAHASAN

A. Karakteristik Responden

Penelitian ini melibatkan 68 responden mahasiswa Program Studi RKS Politeknik Negeri Batam. Karakteristik responden ditinjau dari jenis kelamin, semester yang ditempuh, dan status penyelesaian mata kuliah forensik digital.



Gambar 3. Karakteristik Responden Penelitian

Mayoritas responden berjenis kelamin laki-laki (57,4%) dan berada pada Semester 6 (97,1%), sehingga responden relatif homogen dari sisi angkatan. Sebanyak 83,8% responden sudah menempuh mata kuliah forensik digital,

sedangkan sisanya sedang menempuh mata kuliah tersebut. Karakteristik ini hanya menjadi gambaran umum populasi penelitian dan tidak digunakan untuk analisis perbandingan antar kelompok, sesuai fokus penelitian yang bersifat deskriptif.

B. Hasil Uji Validitas

Uji validitas dilakukan untuk mengetahui apakah setiap butir pernyataan secara tepat mengukur kesadaran forensik digital, menggunakan teknik korelasi Pearson Product Moment (1) antara skor tiap butir dan skor total dari 68 responden. Nilai r hitung dibandingkan dengan r tabel pada taraf signifikansi 5% dan df = n − 2 = 66, yaitu 0,2387 butir dinyatakan valid apabila r hitung > r tabel. Hasil pengujian 24 butir disajikan pada Tabel IV.

TABEL IV HASIL UJI VALIDITAS BUTIR PERNYATAAN

No	Kode	Indikator	Dimensi	r hitung	r tabel	Ket.
1	P1	Identification	Knowledge	0,5873	0,2387	Valid
2	P2	Identification	Knowledge	0,5328	0,2387	Valid
3	P3	Identification	Attitude	0,6129	0,2387	Valid
4	P4	Identification	Attitude	0,4446	0,2387	Valid
5	P5	Identification	Behavior	0,6261	0,2387	Valid
6	P6	Identification	Behavior	0,6616	0,2387	Valid
7	P7	Collection	Knowledge	0,5974	0,2387	Valid
8	P8	Collection	Knowledge	0,6669	0,2387	Valid
9	P9	Collection	Attitude	0,6656	0,2387	Valid
10	P10	Collection	Attitude	0,6832	0,2387	Valid
11	P11	Collection	Behavior	0,6547	0,2387	Valid
12	P12	Collection	Behavior	0,7332	0,2387	Valid
13	P13	Acquisition	Knowledge	0,6575	0,2387	Valid
14	P14	Acquisition	Knowledge	0,7128	0,2387	Valid
15	P15	Acquisition	Attitude	0,6480	0,2387	Valid
16	P16	Acquisition	Attitude	0,4632	0,2387	Valid
17	P17	Acquisition	Behavior	0,7306	0,2387	Valid
18	P18	Acquisition	Behavior	0,7600	0,2387	Valid
19	P19	Preservation	Knowledge	0,7430	0,2387	Valid
20	P20	Preservation	Knowledge	0,6285	0,2387	Valid
21	P21	Preservation	Attitude	0,6510	0,2387	Valid
22	P22	Preservation	Attitude	0,6082	0,2387	Valid
23	P23	Preservation	Behavior	0,6137	0,2387	Valid
24	P24	Preservation	Behavior	0,6338	0,2387	Valid

Seluruh 24 butir memperoleh r hitung lebih besar dari r tabel (0,2387), sehingga semuanya valid dan tidak ada butir yang digugurkan, dengan nilai r hitung berkisar 0,4446–0,7600 yang tersebar merata pada seluruh indikator.

Sebaran nilai r hitung yang merata pada seluruh indikator turut mengindikasikan bahwa tidak ada indikator tertentu yang secara sistematis menghasilkan butir dengan daya beda rendah, sehingga seluruh indikator ISO/IEC 27037 dapat diasumsikan terwakili secara proporsional dalam pengukuran kesadaran forensik digital pada penelitian ini.

C. Hasil Uji Reliabilitas

Uji reliabilitas bertujuan mengetahui konsistensi internal instrumen, dihitung dengan koefisien Alpha Cronbach (2) dari seluruh butir yang valid. Instrumen dinyatakan reliabel apabila nilai Alpha Cronbach ≥ 0,70. Ringkasan hasil pengujian disajikan pada Tabel V.

TABEL V RINGKASAN HASIL UJI RELIABILITAS

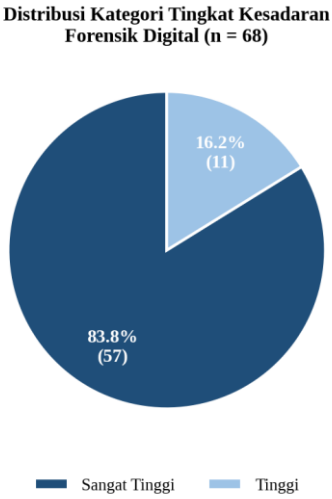
No	Uraian	Nilai
1	Jumlah butir awal	24
2	Jumlah butir valid yang digunakan	24
3	Jumlah butir tidak valid (digugurkan)	0
4	Jumlah varians butir ($\Sigma\sigma_i^2$)	6,8300
5	Varians skor total (σ_t^2)	65,0216
6	Nilai Alpha Cronbach (α)	**0,9339**
7	Keterangan	Reliabel

Seluruh 24 butir valid digunakan dalam penghitungan reliabilitas dan menghasilkan nilai Alpha Cronbach sebesar 0,9339, jauh melampaui ambang 0,70, sehingga instrumen dinyatakan reliabel dengan konsistensi internal yang sangat tinggi.

Tingginya nilai Alpha Cronbach ini turut mengindikasikan bahwa ke-24 butir pernyataan secara konsisten mengukur konstruk yang sama, yaitu kesadaran forensik digital, sehingga skor total maupun skor pada tingkat indikator dan dimensi yang dihasilkan pada bagian selanjutnya dapat digunakan sebagai dasar analisis deskriptif yang andal.

D. Tingkat Kesadaran Forensik Digital Secara Keseluruhan

Analisis deskriptif dilakukan dengan menghitung skor rata-rata jawaban responden (3) terhadap 24 butir valid dan reliabel, yang selanjutnya dikategorikan menggunakan pedoman pada Tabel III. Skor rata-rata keseluruhan dari 68 responden adalah 3,629 (skor individu berkisar 2,667–4,000), termasuk kategori Sangat Tinggi. Distribusi kategori pada tingkat individu disajikan pada Gambar 4



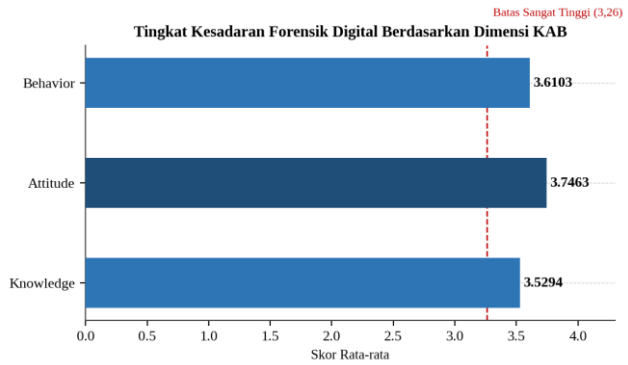
Gambar 4. Distribusi Kategori Tingkat Kesadaran Forensik Digital

Sebanyak 57 responden (83,8%) berada pada kategori Sangat Tinggi dan 11 responden (16,2%) pada kategori Tinggi, tanpa responden pada kategori Rendah maupun Sangat Rendah, menunjukkan tingkat kesadaran forensik digital yang baik secara merata.

Distribusi kategori tersebut turut menegaskan bahwa capaian kesadaran forensik digital yang tinggi bukan hanya dialami oleh sebagian kecil responden, melainkan merata pada hampir seluruh mahasiswa yang menjadi sampel penelitian, sehingga temuan pada tingkat indikator dan dimensi berikutnya dapat diinterpretasikan sebagai gambaran umum populasi dan bukan semata-mata didorong oleh sekelompok kecil responden dengan skor ekstrem.

E. Tingkat Kesadaran Berdasarkan Dimensi Knowledge, Attitude, dan Behavior (KAB)

Tingkat kesadaran forensik digital juga dianalisis berdasarkan tiga dimensi KAB, sebagaimana disajikan pada Gambar 5.

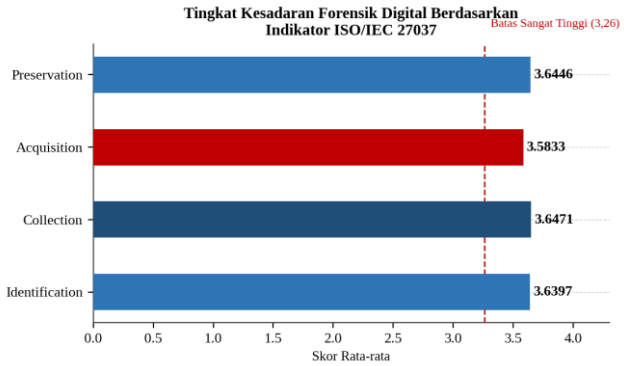


Gambar 5. Tingkat Kesadaran Berdasarkan Dimensi KAB

Dimensi Attitude memperoleh skor tertinggi (3,746), menunjukkan sikap mahasiswa yang sangat positif terhadap pentingnya prosedur forensik digital yang benar. Dimensi Behavior berada di tengah (3,610), menunjukkan penerapan praktik penanganan bukti digital yang sudah cukup baik, sedangkan dimensi Knowledge menjadi yang terendah (3,529), yaitu pemahaman konseptual mahasiswa terhadap tahapan penanganan bukti digital pada setiap indikator ISO/IEC 27037.

F. Tingkat Kesadaran Berdasarkan Indikator ISO/IEC 27037

Tingkat kesadaran forensik digital juga dianalisis berdasarkan empat indikator ISO/IEC 27037, sebagaimana disajikan pada Gambar 6.



Gambar 6. Tingkat Kesadaran Berdasarkan Indikator ISO/IEC 27037

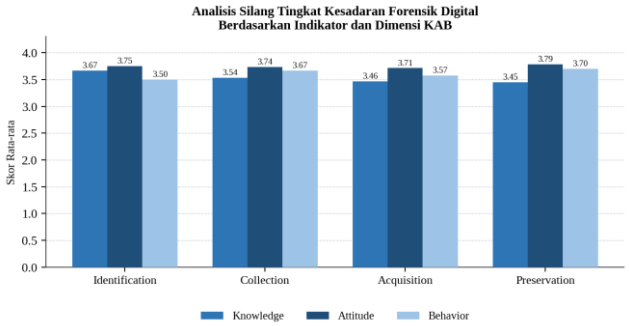
Collection memperoleh skor tertinggi (3,647) di antara keempat indikator, berkaitan dengan pemahaman dan penerapan prosedur pengumpulan bukti digital. Preservation (3,645) dan Identification (3,640) berada pada level yang hampir setara, masing-masing berkaitan dengan cara menjaga keutuhan bukti digital dan kemampuan mengenali jenis perangkat/data yang berpotensi menjadi sumber bukti. Acquisition memperoleh skor terendah (3,583), berkaitan dengan cara menyalin/mengambil data tanpa mengubah keasliannya, tahapan yang menuntut pemahaman teknis lebih mendalam.

G. Analisis Silang Indikator dan Dimensi KAB

Untuk gambaran lebih rinci, dilakukan analisis silang antara empat indikator dan tiga dimensi KAB, dihitung langsung dari 24 butir pernyataan (P1–P24) sehingga setiap sel merupakan rata-rata dua butir. Hasil analisis silang disajikan pada Tabel VI dan Gambar 7.

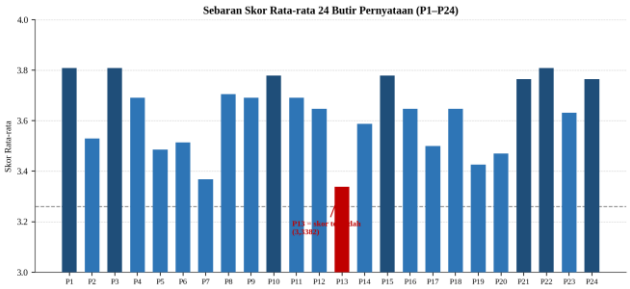
TABEL VI ANALISIS SILANG INDIKATOR DAN DIMENSI KAB

Indikator	Knowledge	Attitude	Behavior	Rata-rata
Identification	3,6691	3,7500	3,5000	3,6397
Collection	3,5368	3,7353	3,6691	3,6471
Acquisition	3,4632	3,7132	3,5735	3,5833
Preservation	3,4485	3,7868	3,6985	3,6446
Rata-rata Dimensi	**3,5294**	**3,7463**	**3,6103**	**3,6287**



Gambar 7. Analisis Silang Skor Indikator dan Dimensi KAB

Skor terendah pada tabel silang ditemukan pada Preservation-Knowledge (3,449) dan Acquisition-Knowledge (3,463), sedangkan skor tertinggi pada Preservation-Attitude (3,787) dan Identification-Attitude (3,750), menunjukkan kelemahan relatif terkonsentrasi pada dimensi Knowledge di tahap Acquisition dan Preservation. Konsisten dengan pola ini, skor terendah dari seluruh 24 butir ditemukan pada butir P13 (Acquisition-Knowledge, mengenai pemahaman cara menyalin data tanpa mengubah keasliannya) sebesar 3,338. Sebaran skor pada tingkat butir (P1–P24) turut memperjelas pola tersebut, sebagaimana disajikan pada Gambar 8 hampir seluruh butir berada pada rentang 3,3–3,8, dengan butir P13 tampak menonjol sebagai satu-satunya titik yang berada di bawah 3,34.



Gambar 8. Sebaran Skor Rata-rata 24 Butir Pernyataan

Pola sebaran skor butir yang relatif homogen, kecuali pada butir P13, mengindikasikan bahwa kelemahan kesadaran forensik digital mahasiswa RKS tidak bersifat menyebar pada banyak aspek, melainkan terkonsentrasi pada satu area teknis yang spesifik, yaitu pemahaman konseptual mengenai proses penyalinan data forensik. Temuan ini memberi implikasi praktis bahwa intervensi peningkatan kesadaran dapat difokuskan secara terarah pada penguatan materi Acquisition, alih-alih melakukan penyesuaian menyeluruh terhadap seluruh materi forensik digital dalam kurikulum.

H. Pembahasan

Tingkat kesadaran forensik digital mahasiswa Program Studi RKS secara keseluruhan berada pada kategori Sangat Tinggi (3,629), diperkuat oleh 83,8% responden berkategori Sangat Tinggi dan sisanya Tinggi, tanpa ada yang berkategori Rendah atau Sangat Rendah. Capaian ini wajar mengingat program studi RKS bersinggungan langsung dengan materi forensik digital, sehingga mahasiswa memperoleh paparan konsep tersebut baik melalui perkuliahan maupun praktik yang relevan dengan bidang keilmuannya.

Seluruh indikator ISO/IEC 27037 berada pada kategori Sangat Tinggi, dengan skor tertinggi pada Collection (3,647) dan terendah pada Acquisition (3,583). Meskipun selisihnya kecil, posisi Acquisition sebagai skor terendah didukung oleh butir P13 yang juga menjadi skor terendah dari seluruh 24 butir (3,338) menggambarkan bahwa tahap akuisisi relatif paling menantang, karena menuntut pemahaman teknis spesifik agar salinan data (image) benar-benar identik dengan sumber tanpa mengubah integritasnya [11]. Sebaliknya, skor tertinggi pada Collection menunjukkan mahasiswa relatif paling menguasai prosedur pengumpulan bukti digital, yang dapat dipahami karena tahap ini umumnya diajarkan secara lebih eksplisit dan berulang dalam perkuliahan dibandingkan tahap akuisisi yang lebih teknis dan spesifik alat.

Ditinjau dari tiga dimensi KAB, Attitude memperoleh skor tertinggi (3,746), diikuti Behavior (3,610), dan Knowledge terendah (3,529), meskipun ketiganya Sangat Tinggi menunjukkan sikap positif mahasiswa sedikit lebih unggul dibandingkan penguasaan pengetahuan teknisnya. Kesenjangan ini terlihat lebih jelas pada tabel silang (Tabel VI) pada indikator Acquisition dan Preservation, skor Knowledge (3,463 dan 3,449) jauh di bawah skor Attitude pada indikator yang sama (3,713 dan 3,787). Artinya, mahasiswa sudah menyadari pentingnya menjaga keaslian dan keutuhan bukti digital, namun pemahaman teknis cara melakukannya belum sepenuhnya sebanding, konsisten dengan butir P13 (Acquisition-Knowledge) sebagai skor terendah dari seluruh butir.

Secara akademik, temuan ini menegaskan bahwa instrumen berbasis empat indikator ISO/IEC 27037 dan tiga dimensi KAB dapat memetakan kesadaran forensik digital secara rinci hingga level butir, sehingga bagian yang relatif lebih lemah dapat diidentifikasi secara spesifik. Secara praktis, temuan bahwa dimensi Knowledge pada indikator Acquisition dan Preservation relatif lebih rendah dapat menjadi masukan bagi pengelola program studi untuk memperkuat materi dan praktikum teknik akuisisi data secara forensically sound serta metode penjagaan bukti digital, misalnya melalui sesi praktik langsung (hands-on) menggunakan perangkat forensik yang umum digunakan [10]. Perlu ditegaskan bahwa penelitian ini bersifat deskriptif dan tidak bertujuan membandingkan tingkat kesadaran antar kelompok responden karakteristik pada Tabel IV hanya menjadi gambaran umum populasi.

Temuan bahwa dimensi Attitude secara konsisten memperoleh skor tertinggi dibandingkan Knowledge sejalan dengan gagasan model KAB yang dikemukakan oleh Kruger & Kearney [5], yang menempatkan Attitude sebagai penghubung antara pengetahuan dan tindakan nyata [9]. Pada konteks forensik digital, tingginya skor Attitude tanpa diimbangi penguasaan Knowledge yang setara

mengindikasikan adanya kesadaran akan pentingnya suatu tindakan tanpa sepenuhnya dibarengi kemampuan teknis untuk melaksanakannya, pola yang juga ditemukan pada konteks keamanan informasi secara umum [6]. Pola ini memperkuat argumen bahwa peningkatan kesadaran keamanan siber maupun forensik digital tidak dapat hanya mengandalkan penanaman nilai normatif tentang pentingnya suatu prosedur, tetapi juga perlu disertai penguatan kompetensi teknis melalui pembelajaran berbasis praktik.

I. Keterbatasan Penelitian

Penelitian ini memiliki beberapa keterbatasan yang perlu dipertimbangkan dalam menginterpretasikan temuan. Pertama, pengukuran kesadaran forensik digital menggunakan instrumen self-report berupa kuesioner tertutup, sehingga skor yang diperoleh mencerminkan persepsi dan pengakuan diri responden, bukan pengukuran langsung terhadap kompetensi teknis atau perilaku aktual mahasiswa saat menangani bukti digital secara nyata. Kedua, sampel penelitian bersifat relatif homogen karena mayoritas responden berasal dari angkatan yang sama (Semester 6), sehingga temuan ini belum tentu menggambarkan kesadaran forensik digital pada mahasiswa di angkatan lain, termasuk mahasiswa yang belum menempuh mata kuliah forensik digital. Ketiga, penelitian ini bersifat deskriptif dan cross-sectional, sehingga tidak dapat menjelaskan hubungan sebab-akibat antar variabel maupun perkembangan kesadaran forensik digital mahasiswa dari waktu ke waktu. Keempat, penelitian ini hanya mencakup empat tahapan awal penanganan bukti digital sebagaimana diatur dalam ISO/IEC 27037, yaitu Identification, Collection, Acquisition, dan Preservation, tanpa menyentuh tahapan analisis dan pelaporan bukti digital yang diatur pada standar terkait lainnya seperti ISO/IEC 27042 dan 27043. Dengan demikian, kesimpulan penelitian ini terbatas pada kesadaran mahasiswa dalam menangani bukti digital sebelum tahap analisis, dan belum dapat digeneralisasi untuk menggambarkan kesadaran mahasiswa pada keseluruhan siklus investigasi forensik digital.

Berdasarkan keterbatasan tersebut, penelitian selanjutnya disarankan mempertimbangkan beberapa hal. Pertama, pengukuran kesadaran dapat dilengkapi dengan metode observasi langsung atau uji berbasis kinerja (performance-based assessment), misalnya melalui simulasi penanganan bukti digital, untuk memvalidasi kesesuaian antara persepsi diri dan kompetensi aktual mahasiswa, khususnya pada tahap Acquisition yang teridentifikasi sebagai area yang relatif lemah pada penelitian ini. Kedua, penelitian lanjutan dapat memperluas cakupan sampel dengan melibatkan mahasiswa dari berbagai angkatan maupun program studi keamanan siber di institusi lain, sehingga temuan dapat digeneralisasi secara lebih luas. Ketiga, desain penelitian longitudinal dapat digunakan untuk mengamati perkembangan kesadaran forensik digital mahasiswa sepanjang masa studi, termasuk mengevaluasi efektivitas intervensi kurikulum seperti penambahan praktikum akuisisi data secara forensically sound terhadap peningkatan dimensi Knowledge yang relatif masih tertinggal dibandingkan Attitude dan Behavior.

IV. KESIMPULAN

Tingkat kesadaran forensik digital mahasiswa Program Studi RKS Politeknik Negeri Batam secara keseluruhan berdasarkan pendekatan KAB berada pada kategori sangat tinggi, dengan skor rata-rata sebesar 3,629 pada rentang 3,26 - 4,00. Pada tingkat indikator ISO/IEC 27037, skor rata-rata Identification, Collection, Acquisition, dan Preservation seluruhnya berada pada kategori sangat tinggi, dengan Acquisition memperoleh skor relatif paling rendah, yang mengindikasikan bahwa kesadaran mahasiswa pada tahapan penyalinan data (imaging) tanpa mengubah keasliannya masih perlu mendapat perhatian lebih dibandingkan tahapan lain.

Pada tingkat dimensi KAB, Attitude memperoleh skor tertinggi, diikuti Behavior, sedangkan Knowledge memperoleh skor terendah meskipun tetap berada pada kategori sangat tinggi. Hasil penelitian ini mengonfirmasi bahwa mahasiswa RKS, yang kurikulumnya telah mencakup mata kuliah Forensik Siber, memiliki bekal kesadaran forensik digital yang lebih baik dibandingkan gambaran kesadaran keamanan siber mahasiswa secara umum. Program studi disarankan memperkuat materi perkuliahan pada aspek teknis penyalinan data (imaging) dan preservasi bukti digital, misalnya melalui praktikum atau simulasi langsung, agar pemahaman teoretis mahasiswa semakin sejalan dengan sikap dan perilaku yang telah baik.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Program Studi Rekayasa Keamanan Siber, Jurusan Teknik Informatika, Politeknik Negeri Batam, serta seluruh mahasiswa yang telah bersedia menjadi responden dalam penelitian ini.

DAFTAR PUSTAKA

[1] Infobanknews, “BSSN Ungkap 5,2 Miliar Anomali Trafik Internet, Mayoritas Berpotensi Jadi Ransomware,” Infobanknews, Mei 8, 2026. [Online]. Tersedia: https://infobanknews.com/bssn-ungkap-52-miliar-anomali-trafik-internet-mayoritas-berpotensi-jadi-ransomware

[2] D. Humaira, N. A. Fazlasya, S. Alwi, and P. H. Tafonao, “Analisis Dampak Human Error Terhadap Kebocoran Data Pribadi di Kalangan Pengguna Digital,” Jurnal Ilmu Komputer dan Manajemen (JIKUM), vol. 2, no. 2, pp. 203–206, Nov. 2026.

[3] Z. Morić, V. Dakić, and I. Ogrizek Biškupić, “An empirical assessment of digital forensic process reliability using integrated ISO/IEC 27037 and 27041 standards,” J. Cybersecur. Priv., vol. 6, no. 2, p. 57, Mar. 2026, doi: 10.3390/jcp6020057.

[4] T. Tan, H. Sama, T. Wibowo, G. Wijaya, and O. E. Aboagye, “Kesadaran Keamanan Siber pada Kalangan Mahasiswa Universitas di Kota Batam,” Jurnal Teknologi dan Informasi (JATI), vol. 14, no. 2, pp. 163–173, 2024, doi: 10.34010/jati.v14i2.12518.

[5] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," Computers & Security, vol. 25, no. 4, pp. 289–296, 2006, doi: 10.1016/j.cose.2006.02.008.

[6] F. Arum, A. Zubaidi, and R. B. Huwae, "Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan HAIS-Q: Mengungkap Kesenjangan antara Sikap dan Pengetahuan Mahasiswa," Jurnal Bumigora Information Technology (BITe), vol. 7, no. 2, pp. 83–94, 2025, doi: 10.30812/bite.v7i2.5430.

[7] Politeknik Negeri Batam, "Publikasi Kurikulum Program Studi D4 Rekayasa Keamanan Siber," Polibatam, Batam, 2024. [Online]. Tersedia: https://www.polibatam.ac.id/wp-content/uploads/2021/10/Publikasi-Kurikulum-RKS-v2024.pdf

[8] J. Parhusip, F. U. H. Zahra, A. Monalisa, M. R. Kurniawan, and N. P. Lowryanty, "Analisis Tingkat Kesadaran Mahasiswa terhadap Keamanan Data Pribadi di Era Digital: Studi Komparatif antara Mahasiswa Teknik Informatika dan Non-Teknik Informatika," RIGGS: Journal of Artificial Intelligence and Digital Business, vol. 4, no. 4, pp. 8091–8101, 2026, doi: 10.31004/riggs.v4i4.4516.

[9] B. Ahamed, M. R. H. Polas, A. I. Kabir, A. S. Md. Sohel-Uz-Zaman, A. Al Fahad, S. Chowdhury, and M. R. Dey, "Empowering Students for Cybersecurity Awareness Management in the Emerging Digital Era: The Role of Cybersecurity Attitude in the 4.0 Industrial Revolution Era," SAGE Open, vol. 14, 2024, doi: 10.1177/21582440241228920.

[10] Z. D. A. Maulana, M. P. Aji, A. P. Wicaksono, and Harjono, "Digital Forensics Implementation on CCTV Using ISO/IEC 27037 and ISO/IEC 27042," Jurnal E-Komtek, vol. 9, no. 2, pp. 421–433, 2025, doi: 10.37339/e-komtek.v9i2.2920.

[11] H. S. Alawi, I. Riadi, and Sunardi, "Improving Credibility of Digital Evidence Investigation in E-Commerce Fraud Cases using ISO/IEC 27037," International Journal of Advances in Data and Information Systems, vol. 6, no. 2, pp. 479–495, 2025, doi: 10.59395/ijadis.v6i2.1408.