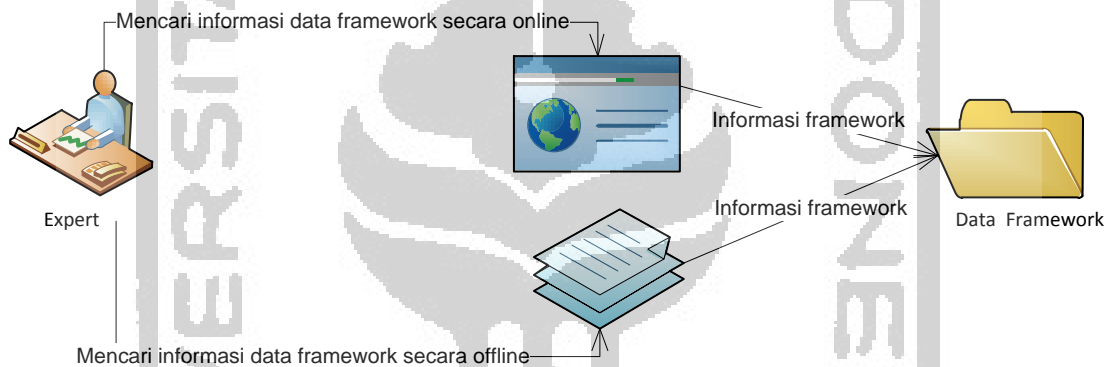


BAB 4

Hasil dan Pembahasan

Penelitian ini berawal dari belum adanya sebuah repository yang mendokumentasikan framework forensika digital. Framework forensika digital masih tersebar dalam berbagai *paper*, sehingga investigator harus mencari informasi framework forensika digital satu persatu. Ini tentunya tidak praktis dan menghambat investigator dalam memulai melakukan investigasi untuk sebuah kasus. Dengan adanya repository ini, diharapkan akan membantu investigator (sebagai *expert*) untuk menghemat waktu mengumpulkan informasi mengenai framework forensika digital. Alur kerja *expert* (dalam hal ini adalah investigator) sebelum ada sistem repository sebagaimana ditunjukkan oleh Gambar 4.1.



Gambar 4.1 Alur Kerja *Expert* Sebelum Adanya Sistem *Repository*

Langkah pertama adalah membuat perancangan sistem, mulai dari database, software maupun hardware yang akan digunakan, alur program. Setelah membuat perancangan sistem, langkah selanjutnya adalah mengimplementasikan dalam sebuah sistem repository. Pada penelitian ini, implementasi dilakukan dengan membuat sebuah aplikasi repository dan evaluasi framework forensika digital menggunakan Daubert Criteria berbasis website. Website ini digunakan untuk melakukan simulasi mendokumentasikan dan memberikan evaluasi framework forensika digital yang telah dibuat. Dalam website ini, *user* dibedakan menjadi tiga, yaitu *user* sebagai umum, *admin* dan *expert*.

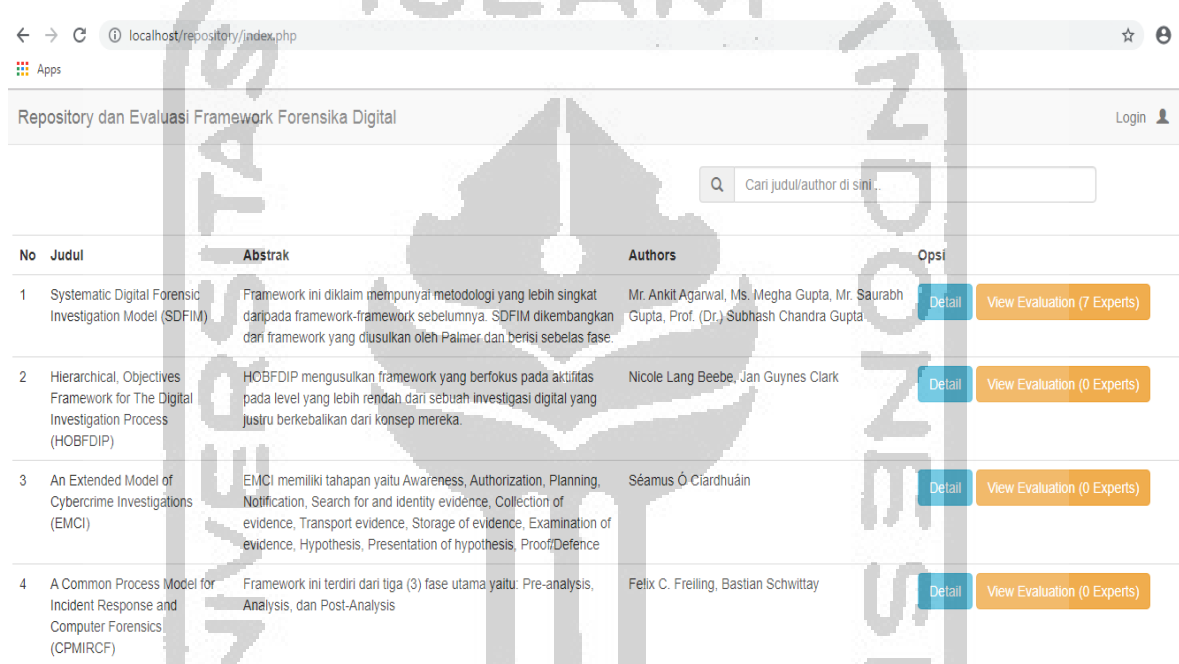
Pembagian hak akses untuk tiap pengguna (umum, admin, dan *expert*) adalah sebagai berikut:

1. Umum

- ❖ View data framework

- ❖ View resume hasil evaluasi framework
2. Admin
 - ❖ Entri, edit, dan hapus data framework
 - ❖ Entri, edit, dan hapus data expert
 3. Expert
 - ❖ Evaluasi framework
 - ❖ View data framework

Berikut adalah tampilan dashboard dari website yang dibuat sebagaimana ditunjukkan oleh Gambar 4.2.



Gambar 4.2 Dashboard Website

Setiap framework akan memberikan informasi jumlah expert yang sudah memberikan evaluasi. Untuk melakukan entri data framework yang baru, admin hanya perlu mengisi data sebagaimana ditunjukkan oleh Gambar 4.3.

Gambar 4.3 Halaman Entri Framework

Sementara itu, data framework forensika digital yang ditampilkan adalah sebagai berikut:

- ❖ Judul, yang menunjukkan nama framework forensika digital. Jika tidak ada nama framework, maka dapat diisi dengan judul penelitian yang mengusulkan framework tersebut.
- ❖ Abstrak, yang berisi uraian singkat mengenai framework forensika digital.
- ❖ Author, yang berisi nama-nama peneliti yang mengusulkan framework forensika digital.
- ❖ Tahun, yang menunjukkan tahun terbit jurnal yang mengusulkan framework tersebut.
- ❖ Jurnal, berisi daftar berbagai jurnal yang terkait dengan framework yang diusulkan. Jurnal yang menjadi acuan dari framework yang diusulkan perlu disebutkan.
- ❖ Tahapan, berisi gambar yang menunjukkan tahapan proses investigasi forensika digital yang diusulkan oleh framework.
- ❖ PDF File, berisi file naskah publikasi dari penelitian yang mengusulkan framework tersebut.

Informasi framework forensika digital yang lebih lengkap bisa dilihat di Detail Framework, sebagaimana ditunjukkan oleh Gambar 4.4.

Detail Framework

[← Kembali](#)

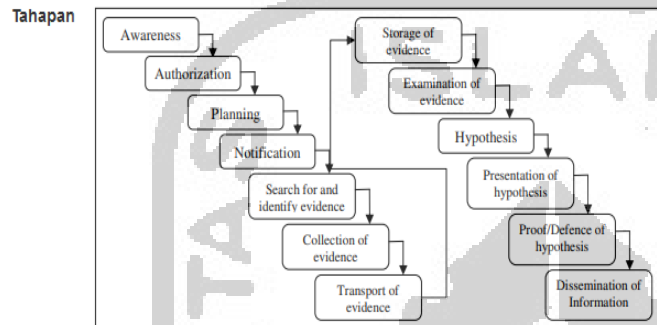
Judul An Extended Model of Cybercrime Investigations (EMCI)

Abstrak EMCI memiliki tahapan yaitu Awareness, Authorization, Planning, Notification, Search for and identify evidence, Collection of evidence, Transport evidence, Storage of evidence, Examination of evidence, Hypothesis, Presentation of hypothesis, Proof/Defence

Author Séamus Ó Ciardhuáin

Tahun 2004

Jurnal 1. Reith, M., Carr, C. and Gunsch, G. (2002). 'An xamination of Digital Forensic Models', International Journal of Digital Evidence, 1(3), pp. 1-12.
2. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd edn. New York: Elsevier Academic Press.



PDF File [Download](#)

Gambar 4.4 Contoh Halaman Detail Framework

Daftar framework forensika digital yang sudah dimasukkan kedalam *repository* sebagai berikut.

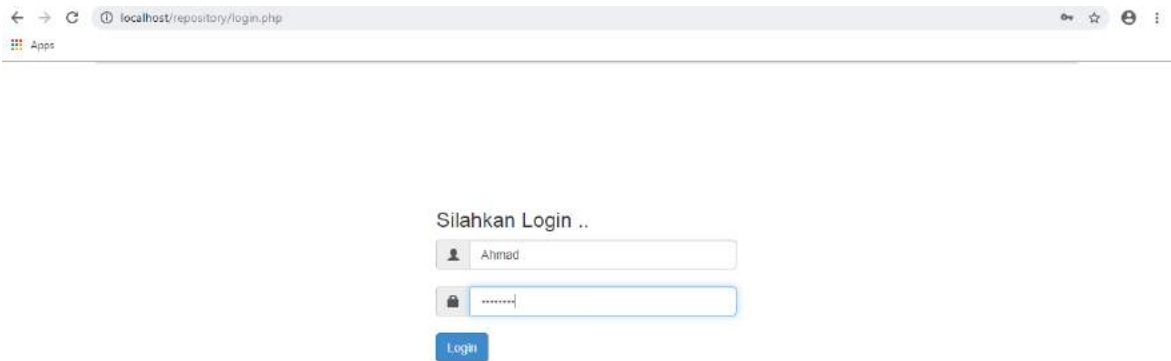
Tabel 4.1 Daftar Framework Forensika Digital didalam *Repository*

No	Judul	Author
1	<i>Systematic Digital Forensic Investigation Model (SDFIM)</i>	Mr. Ankit Agarwal, Ms. Megha Gupta, Mr. Saurabh Gupta, Prof. (Dr.) Subhash Chandra Gupta
2	<i>Hierarchical, Objectives Framework for The Digital Investigation Process (HOBFDIP)</i>	Nicole Lang Beebe, Jan Guynes Clark
3	<i>An Extended Model of Cybercrime Investigations (EMCI)</i>	Séamus Ó Ciardhuáin
4	<i>A Common Process Model for Incident Response and Computer Forensics (CPMIRCF)</i>	Felix C. Freiling, Bastian Schwittay
5	<i>Four Step Forensic Process (FSFP)</i>	Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang
6	<i>Integrated Digital Forensic Process Model (IDFPM)</i>	Michael Donovan Kohn
7	<i>Digital Evidence Cabinets (DEC)</i>	Yudi Prayudi, Ahmad Ashari, Tri K Priyambodo
8	<i>Computer Forensics Field Triage Process Model (CFFTPM)</i>	Marcus K. Rogers, James Goldman, Rick Mislán, Timothy Wedge, Steve Debrotá
9	<i>Mapping Process of Digital Forensic Investigation Framework (MPDFIF)</i>	Siti Rahayu Selamat, Robiah Yusof, Shahrin Sahib

10	<i>Abstract Digital Forensics Model (ADFM)</i>	M. Reith, C. Carr dan G. Gunsh
11	<i>The Integrated Digital Investigation Process (IDIP)</i>	B. Carrier, E. Spafford
12	<i>The Digital Forensics Research Workshop Model (DFRWS)</i>	Palmer
13	<i>A Forensic Framework for Tracing Phishers</i>	Sebastian Gajek, Ahmad Reza Sadegh
14	<i>A Framework for the Forensic Investigation of Unstructured Email Relationship Data</i>	John Haggerty, Alexander J. Karran, David J. Lamb, Mark J. Taylor
15	<i>A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia</i>	Yudi Prayudi, Ahmad Ashari, Tri K. Priyambodo
16	<i>Computer Forensic Investigative Process</i>	Mark M. Politt
17	<i>Enhanced Digital Investigation Process Model (EDIP)</i>	V. Baryamereeba & F. Tushabe
18	<i>Digital Forensic Model based on Malaysian Investigation Process (DFMMIP)</i>	Perumal Sundresan
19	<i>End to End Digital Investigation</i>	P. Stephenson
20	<i>Dual Data Analysis Process (DDAP)</i>	D. Bem & E. Huebner
21	<i>Network Forensic Generic Process Model (NFGP)</i>	Emmanuel S. Pilli , R.C. Joshi , Rajdeep Niyogi
22	<i>Evidence Analysis Framework</i>	Abdullah AlShaikh, Mohamed Sedky
23	<i>Digital Forensic Investigation Model</i>	Inikpi O. Ademu, Dr Chris O. Imafidon, Dr David S. Preston

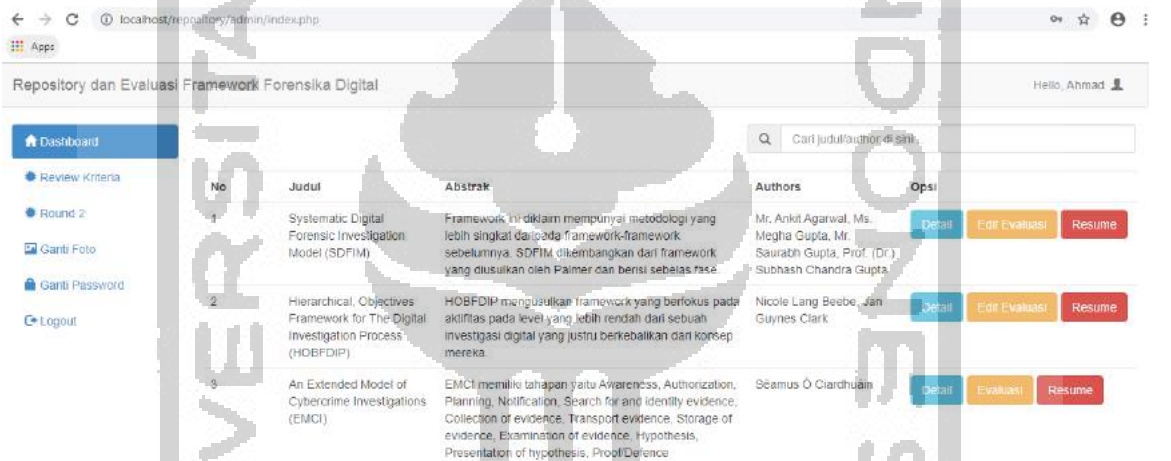
Setelah repository sudah jadi, selanjutnya expert (dalam hal ini adalah investigator) sudah dapat memberikan evaluasi. Evaluasi framework forensika digital menggunakan Daubert Criteria menjadi penting karena Daubert Criteria sudah banyak diterapkan di persidangan. Barang bukti digital harus dapat dibuktikan secara ilmiah, dan bukanlah *junk science*. Untuk mendapatkan barang bukti yang dapat diterima di pengadilan, barang bukti haruslah melewati proses investigasi dengan menggunakan framework forensika digital yang sesuai dengan kriteria Daubert. Karena inilah dibutuhkan evaluasi framework forensika digital. Hasil evaluasi belum dapat diambil kesimpulan, karena Daubert Criteria mempunyai tingkat prioritas yang berbeda. Dibutuhkan Delphi Method untuk mendapatkan kesimpulan yang berupa konsensus (menunjukkan berapa kriteria Daubert yang dipenuhi oleh sebuah framework forensika digital).

Seorang *expert* (dalam hal ini adalah investigator) dapat melakukan login (setelah sebelumnya dibuatkan akun oleh admin) untuk melakukan evaluasi framework forensika digital sebagaimana ditunjukkan oleh Gambar 4.5.



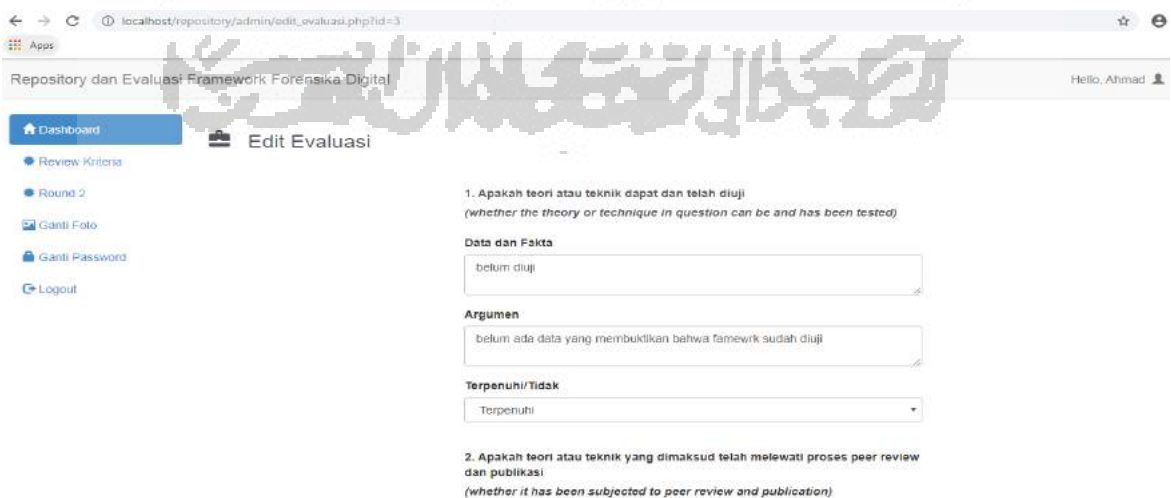
Gambar 4.5 Halaman Login

Dari banyaknya framework forensika digital yang ada di repository, expert dapat memilih framework apa yang akan diberikan evaluasi sebagaimana ditunjukkan oleh Gambar 4.6.



Gambar 4.6 Halaman Dashboard Expert

Evaluasi sebuah framework forensika digital diberikan untuk masing-masing kriteria sebagaimana ditunjukkan oleh Gambar 4.7, Gambar 4.8, Gambar 4.9, dan Gambar 4.10.



Gambar 4.7 Halaman Evaluasi Framework

← → C localhost/repository/admin/edit_evaluasi.php?id=3 ☆ e

Apps

Data dan Fakta
sudah ada paper terpublikasi yang merujuk pada framework ini

Argumen
paper yang merujuk ke framework ini menunjukkan bahwa framework sudah melalui peer review dan publikasi

Terpenuhi/Tidak
Terpenuhi

3. Apakah teori atau teknik yang dimaksud diketahui potensi kesalahannya (its known or potential error rate)

Data dan Fakta
belum diketahui

Argumen
framework belum pernah diuji sehingga belum diketahui berapa letak kesalahannya

Terpenuhi/Tidak
Terpenuhi

Gambar 4.8 Halaman Evaluasi Framework Lanjutan1

← → C localhost/repository/admin/edit_evaluasi.php?id=3 ☆ e

Apps

4. Adanya standard yang melakukan kontrol terhadap pengoperasiannya (the existence and maintenance of standards controlling its operation)

Data dan Fakta
tidak ada

Argumen
framework merujuk pada ACPPI tetapi tidak ada satupun yang diterapkan pada tahapan framework yang diusulkan

Terpenuhi/Tidak
Terpenuhi

5. Apakah memungkinkan untuk diterima secara luas oleh komunitas ilmiah yang relevan (whether it has attracted widespread acceptance within the relevant scientific community)

Data dan Fakta
framework sudah diterima oleh para expert

Argumen
sudah banyak expert yang menetakan dan memberikan feedback terkait framework ini

Terpenuhi/Tidak
Terpenuhi

Simpan

Gambar 4.9 Halaman Evaluasi Framework Lanjutan2

Gambar 4.10 Halaman Evaluasi Framework Lanjutan3

Setelah sebuah framework dievaluasi minimal oleh tiga expert, maka admin akan melakukan pengecekan hasil evaluasi. Hasil evaluasi awal ini akan masuk ke Round 1 dari Delphi Method. Dari lima kriteria dalam Daubert, admin akan melakukan pengecekan apakah ada kriteria dengan hasil evaluasi yang berbeda dari masing-masing expert. Hasil evaluasi Round 1 sebagaimana ditunjukkan oleh Gambar 4.11.

SME	Kriteria 1	Kriteria 2	Kriteria 3	Kriteria 4	Kriteria 5	Total
Ahmad	Tidak	Terpenuhi	Tidak	Terpenuhi	Tidak	
Jon Snow	Tidak	Terpenuhi	Tidak	Tidak	Tidak	
Momonosuke	Tidak	Terpenuhi	Tidak	Terpenuhi	Tidak	
HASIL	Tidak (Konvergen)	Terpenuhi (Konvergen)	Tidak (Konvergen)	Divergen	Tidak (Konvergen)	1/5

Kriteria 1: Apakah teori atau teknik dapat dan telah diuji.
Kriteria 2: Apakah teori atau teknik yang dimaksud telah melewati proses peer review dan publikasi.
Kriteria 3: Apakah teori atau teknik yang dimaksud diketahui potensi kesalahannya.
Kriteria 4: Adanya standard yang melakukan kontrol terhadap pengoperasiannya.
Kriteria 5: Apakah memungkinkan untuk diterima secara luas oleh komunitas ilmiah yang relevan.

Gambar 4.11 Contoh Hasil Evaluasi Framework Round 1

Dari Gambar 4.11 diketahui bahwa dari tiga expert (Ahmad, Jon Snow, dan Momonosuke) mempunyai pendapat yang berbeda mengenai kriteria keempat, yaitu “Adanya standard yang melakukan control terhadap pengoperasiannya (*the existence and maintenance of standards controlling its operation*)”. Expert Ahmad dan Momonosuke berpendapat bahwa framework tersebut sudah cukup memenuhi kriteria keempat, sedangkan expert Jon Snow berpendapat bahwa framework tersebut belum memenuhi kriteria keempat. Karena adanya perbedaan pendapat diantara expert (masih ada kriteria yang divergen), maka admin memberikan notifikasi pada ketiga expert untuk memberikan evaluasi ulang khusus untuk kriteria keempat. Notifikasi akan muncul ketika expert melakukan login ke sistem, sebagaimana ditunjukkan oleh Gambar 4.12.

Notification

Silahkan melakukan evaluasi ulang framework dimenu Review Kriteria!

No	Judul	Detail	Author di sini	Opsi
1	Systematic Digital Forensic Investigation Model (SDFIM)	Framework ini diklaim mempunyai metodologi yang lebih singkat daripada framework-framework sebelumnya. SDFIM dikembangkan dari framework yang diusulkan oleh Palmer dan berisi sebelas fase	Mr. Ankit Agarwal, Ms. Megha Gupta, Mr. Saurabh Gupta, Prof. (Dr.) Subhash Chandra Gupta	Detail Edit Evaluasi Resume
2	Hierarchical, Objectives Framework for The Digital Investigation Process (HOBFDIP)	HOBFDIP mengusulkan framework yang berfokus pada aktifitas pada level yang lebih rendah dan sebuah investigasi digital yang justru berkebalikan dari konsep mereka.	Nicole Lang Beebe, Jan Guynes Clark	Detail Edit Evaluasi Resume

Gambar 4.12 Notifikasi Untuk Review Kriteria Ulang

Selanjutnya, *expert* akan diarahkan ke menu Review Criteria untuk melakukan evaluasi ulang pada kriteria keempat, sebagaimana ditunjukkan oleh Gambar 4.13.



Gambar 4.13 Contoh Menu Review Kriteria

Admin dapat melakukan pengecekan apakah semua expert sudah melakukan evaluasi ulang. Setelah Admin memastikan bahwa semua expert sudah melakukan evaluasi ulang, maka Admin akan melakukan pengecekan hasil evaluasinya. Jika semua expert mempertahankan evaluasi (yang berarti hasil evaluasi tidak berubah), maka Admin akan melakukan voting. Karena pada hasil evaluasi framework tersebut diketahui bahwa jumlah expert yang berpendapat bahwa framework memenuhi kriteria keempat dari Daubert (Terpenuhi vs Tidak = 2 vs 1), maka Admin membuat kesimpulan bahwa framework tersebut memenuhi kriteria keempat dari Daubert. Selanjutnya Admin memberikan klik pada tombol "Publish" untuk menampilkan resume hasil evaluasi pada Dashboard.

Untuk contoh kasus framework tersebut, dari resume hasil evaluasi diketahui bahwa hasil dari *Daubert Scoring* adalah 2/5. Artinya hasil konsensus menunjukkan bahwa framework tersebut memenuhi dua kriteria Daubert yaitu peer review dan standard control. Contoh hasil konsensus sebagaimana ditunjukkan oleh Gambar 4.14.

Repository dan Evaluasi Framework Forensika Digital Hello, admin

Experts	Kriteria 1	Kriteria 2	Kriteria 3	Kriteria 4	Kriteria 5	Total
Ahmad	Tidak	Terpenuhi	Tidak	Terpenuhi	Tidak	
Jon Snow	Tidak	Terpenuhi	Tidak	Tidak	Tidak	
Momonosuke	Tidak	Terpenuhi	Tidak	Terpenuhi	Tidak	
HASIL:	Tidak (Konvergen)	Terpenuhi (Konvergen)	Tidak (Konvergen)	Terpenuhi (VOTE)	Tidak (Konvergen)	2/5

Kriteria 1: Apakah teori atau teknik dapat dan telah diuji.
Kriteria 2: Apakah teori atau teknik yang dimaksud telah melewati proses peer review dan publikasi.
Kriteria 3: Apakah teori atau teknik yang dimaksud diketahui potensi kesalahannya.
Kriteria 4: Adanya standard yang melakukan kontrol terhadap pengoperasiannya.
Kriteria 5: Apakah memungkinkan untuk diterima secara luas oleh komunitas ilmiah yang relevan.

Gambar 4.14 Contoh Hasil Konsensus

Dari uraian diatas diketahui bahwa sistem repository dan evaluasi framework forensika digital dapat melakukan hal seperti:

1. Sistem dapat membuat repository framework (melakukan entri, update, maupun hapus data framework).
2. Sistem dapat untuk memberikan evaluasi framework forensika digital menggunakan *Daubert Criteria*. Namun resume hasil evaluasi tidak muncul pada tiap framework, karena harus ada minimal tiga expert yang memberikan evaluasi. Setelah itu Admin akan melakukan pengecekan pada hasil Round 1, apakah ada kriteria yang belum konvergen (masih divergen). Kalau semua kriteria sudah konvergen semua, maka sudah mendapatkan konsensus. Namun jika masih ada kriteria yang konvergen, maka Admin akan memberikan notifikasi pada expert untuk melakukan evaluasi ulang. Hasil evaluasi ulang ini akan dilakukan pengecekan oleh Admin. Selanjutnya Admin yang akan melakukan menampilkan hasil resume pada Dashboard.
3. Sistem dapat menampilkan resume hasil evaluasi, yang sudah ditampilkan oleh Admin pada Dashboard.

Dengan adanya evaluasi sistem seperti yang sudah diuraikan, dapat disimpulkan bahwa sistem yang dibuat sudah memenuhi apa saja yang dibutuhkan oleh investigator. Framework forensika digital sudah dapat didokumentasikan dalam sebuah wadah, dan evaluasi framework forensika digital menggunakan *Daubert Criteria* juga dapat diselesaikan.