



Webinar dan Workshop Digital Forensics Berbasis Kali Linux untuk Recovery dan Analisis File Terhapus

Adrian Mustafa¹, Apri Baroka², Muhammad Farhat Nirwansyah³, Nur Fauzta Putra Pratama⁴, Khalisah Hasna Naila Shifa⁵, Rita Dewi Risanty⁶, Hendra⁷, Nurvelly Rosanti⁸, Mirza Sutrisno⁹, Sitti Nurbaya Ambo¹⁰

¹⁻¹⁰ Universitas Muhammadiyah Jakarta

e-mail corespondensi*: 23040700006@student.umj.ac.id

History Article	Abstract
Received: 10 July 2026 Revised: 20 August 2026 Accepted: 29 August 2026	The increasing use of digital storage has created a growing need for basic digital forensics literacy, particularly in understanding the recovery and analysis of deleted files. This community service activity aimed to provide participants with conceptual understanding and practical experience in digital forensics through a webinar and workshop using Kali Linux. The activity was conducted online on 4 July 2026 in collaboration with the Informatics Student Association of Universitas Komputer Indonesia (HMIF UNIKOM). The activity involved 20 active participants from 34 registered participants and consisted of three stages: preparation, implementation, and evaluation. The implementation included delivery of digital forensics materials, guided hands-on practice using Kali Linux with The Sleuth Kit (TSK) and Foremost, and interactive discussion. Evaluation was conducted using pre-test and post-test instruments to assess participants' understanding and a questionnaire to evaluate the implementation of the activity. The results showed an increase in the percentage of correct answers from the pre-test to the post-test, with most post-test items achieving 90–100% correct responses. The participant feedback also indicated positive perceptions of the materials, presenters, and overall implementation. These results indicate that the combination of conceptual material and guided practical activities can support the delivery of basic digital forensics knowledge and practical experience in recovering and analyzing deleted files.
Keyword <i>Digital Forensics; Kali Linux; File Recovery; Deleted Files; Forensic Analysis</i>	

To cite this article: Mustafa, A. et. al. (2026). *Webinar dan Workshop Digital Forensics Berbasis Kali Linux untuk Recovery dan Analisis File Terhapus*. **Kenduri: Jurnal Pengabdian Dan Pemberdayaan Masyarakat**, 6(2) 2026, 357-367. <https://doi.org/10.62159/kenduri.v6i.xxx>

PENDAHULUAN

Perkembangan teknologi informasi telah meningkatkan penggunaan media penyimpanan digital dalam berbagai aktivitas, termasuk pendidikan, pemerintahan, dan dunia usaha. Peningkatan penggunaan data digital juga diikuti oleh kebutuhan untuk menjaga, memeriksa, dan menganalisis informasi digital ketika terjadi kehilangan atau insiden keamanan. Dalam konteks investigasi digital, proses pemeriksaan perlu dilakukan secara sistematis melalui tahapan identifikasi, pengumpulan atau akuisisi, pemeriksaan, analisis, dan pelaporan bukti digital.

Salah satu permasalahan yang relevan dalam digital forensics adalah keberadaan data yang telah dihapus. Penghapusan file tidak selalu menyebabkan seluruh informasi terkait file tersebut hilang dari media penyimpanan. Dalam kondisi tertentu, artefak atau bagian data yang telah dihapus masih dapat ditemukan

dan dipulihkan melalui teknik forensik tertentu. NIST menjelaskan bahwa proses recovery deleted data dapat memungkinkan pemulihan file secara utuh maupun sebagian, tetapi hasil recovery juga memiliki keterbatasan, seperti kemungkinan ditemukannya data yang tidak relevan atau hasil yang tidak lengkap (Lyle et al., 2022).

Proses recovery dalam digital forensics dapat memanfaatkan informasi sistem berkas maupun teknik yang digunakan untuk menemukan kembali data yang tidak lagi tercatat secara normal pada sistem berkas. The Sleuth Kit (TSK), misalnya, merupakan kumpulan perangkat open source untuk analisis sistem berkas dan disk image yang menyediakan fungsi untuk pemeriksaan struktur sistem berkas, data unit, metadata, dan informasi nama file. NIST juga mengategorikan deleted file recovery sebagai salah satu fungsi dalam teknologi dan teknik computer forensics, yaitu pemeriksaan metadata sistem berkas untuk mengidentifikasi file yang telah dihapus dan mencoba melakukan rekonstruksi atau pemulihannya.

Salah satu lingkungan yang dapat digunakan untuk memperkenalkan konsep dan proses digital forensics adalah Kali Linux. Dokumentasi resmi Kali Linux menunjukkan bahwa distribusi tersebut menyediakan berbagai perangkat yang dapat digunakan untuk kebutuhan keamanan dan forensik, serta menyediakan dokumentasi dan informasi penggunaan untuk setiap perangkat yang tersedia. Penggunaan perangkat open source dalam kegiatan edukatif memberikan kesempatan bagi peserta untuk mengenali proses pemeriksaan data digital tanpa harus bergantung pada perangkat lunak komersial. Dalam konteks pembelajaran, The Sleuth Kit juga secara eksplisit dikembangkan sebagai perangkat analisis file dan volume system forensics yang bersifat open source serta memiliki tujuan pendidikan.

Meskipun konsep digital forensics dapat dipelajari melalui materi teoritis, proses pemeriksaan dan recovery data memiliki tahapan teknis yang lebih mudah dipahami apabila disertai dengan visualisasi proses secara langsung. Pendekatan demonstrasi dapat digunakan untuk memperlihatkan bagaimana konsep yang dijelaskan diterapkan pada skenario pemeriksaan media penyimpanan, mulai dari identifikasi media, pemeriksaan sistem berkas, proses recovery, hingga pengamatan terhadap hasil pemulihan. Pendekatan ini juga memungkinkan peserta mengikuti proses pemeriksaan tanpa harus menggunakan data pribadi atau melakukan investigasi terhadap perangkat yang sebenarnya.

Berdasarkan kebutuhan tersebut, kegiatan pengabdian kepada masyarakat ini dilaksanakan dalam bentuk webinar dan workshop digital forensics berbasis Kali Linux bekerja sama dengan Himpunan Mahasiswa Informatika Universitas Komputer Indonesia (HMIF UNIKOM). Kegiatan menggabungkan penyampaian materi konseptual, demonstrasi langsung, dan diskusi mengenai recovery serta analisis file terhapus. Demonstrasi menggunakan Kali Linux dengan perangkat The Sleuth Kit (TSK) dan Foremost untuk memperlihatkan proses identifikasi media penyimpanan, pemulihan file, dan analisis hasil recovery pada skenario kehilangan file. Kegiatan ini bertujuan memberikan pemahaman dasar mengenai digital forensics serta memperkenalkan proses recovery dan analisis file terhapus melalui demonstrasi yang dapat diikuti oleh peserta.

METODE

Kegiatan pengabdian kepada masyarakat dilaksanakan dalam bentuk webinar dan workshop yang menggunakan pendekatan demonstrasi langsung (live demonstration). Pendekatan ini dipilih untuk memperkenalkan konsep dan tahapan dasar digital forensics melalui visualisasi proses recovery dan analisis file terhapus menggunakan Kali Linux. Kegiatan dilaksanakan secara daring dan melibatkan peserta dari kalangan mahasiswa serta masyarakat umum. Pelaksanaan kegiatan terdiri atas tiga tahap utama, yaitu persiapan, pelaksanaan, dan evaluasi.

Tahap persiapan dilakukan melalui koordinasi antara tim pelaksana dan mitra, yaitu Himpunan Mahasiswa Informatika Universitas Komputer Indonesia (HMIF UNIKOM). Persiapan meliputi penyusunan materi digital forensics, penyiapan skenario demonstrasi recovery file terhapus, konfigurasi lingkungan Kali Linux, penyiapan perangkat forensik yang digunakan, serta penyusunan instrumen evaluasi. Materi disusun agar peserta memperoleh pengenalan mengenai konsep digital forensics sebelum mengikuti demonstrasi teknis mengenai proses recovery dan analisis file terhapus.

Tahap pelaksanaan terdiri atas sesi webinar dan workshop. Sesi webinar digunakan untuk menyampaikan konsep dasar digital forensics, karakteristik bukti digital, serta pengenalan terhadap proses recovery file terhapus. Setelah penyampaian materi, kegiatan dilanjutkan dengan workshop berupa demonstrasi langsung oleh narasumber menggunakan Kali Linux. Demonstrasi memperlihatkan alur pemeriksaan media penyimpanan, identifikasi file yang telah dihapus, proses recovery, dan pengamatan terhadap hasil pemulihan. Peserta mengikuti demonstrasi secara daring dan diberikan kesempatan untuk mengajukan pertanyaan serta mendiskusikan tahapan yang ditampilkan.

Demonstrasi dilakukan menggunakan lingkungan Kali Linux dengan perangkat The Sleuth Kit (TSK) dan Foremost. Kali Linux digunakan sebagai lingkungan sistem untuk menjalankan perangkat forensik, sedangkan TSK digunakan untuk memperkenalkan pemeriksaan struktur dan informasi sistem berkas serta file terhapus. Foremost digunakan dalam demonstrasi proses pemulihan berbasis karakteristik data. Pemilihan tools ditujukan untuk memperlihatkan kepada peserta tahapan dasar recovery dan analisis file pada skenario kehilangan data.

Dari aspek etika dan legalitas, seluruh proses demonstrasi menggunakan berkas image bukti elektronik (evidence_ss1.E01) yang merupakan data latihan resmi yang disediakan oleh mentor narasumber untuk keperluan pembelajaran, bukan data milik pihak ketiga yang diperoleh tanpa izin. Kegiatan ini tidak melibatkan akses terhadap perangkat maupun data pribadi milik peserta atau pihak lain mana pun, dan seluruh teknik recovery yang didemonstrasikan ditekankan penggunaannya semata-mata untuk kepentingan edukasi serta investigasi digital yang sah secara hukum.

Peserta kegiatan berjumlah 34 orang yang melakukan pendaftaran, sedangkan 20 peserta tercatat sebagai peserta aktif dalam pelaksanaan dan evaluasi kegiatan. Peserta berasal dari mahasiswa dan masyarakat umum dengan latar belakang yang beragam. Analisis hasil evaluasi dilakukan terhadap peserta yang mengikuti rangkaian evaluasi sehingga jumlah sampel yang digunakan dalam analisis adalah 20 peserta.

Evaluasi pemahaman peserta dilakukan menggunakan pre-test dan post-test yang diberikan sebelum dan setelah kegiatan. Instrumen digunakan untuk mengetahui perubahan tingkat pemahaman peserta terhadap materi digital forensics dan recovery file terhapus. Hasil jawaban dihitung berdasarkan persentase jawaban benar pada setiap butir soal dan dibandingkan antara hasil pre-test dan post-test.

Evaluasi pelaksanaan kegiatan dilakukan melalui kuesioner yang diberikan setelah kegiatan. Kuesioner digunakan untuk memperoleh tanggapan peserta terhadap aspek materi, penyampaian narasumber, pelaksanaan kegiatan, dan manfaat kegiatan. Data kuesioner dianalisis secara deskriptif untuk menggambarkan kecenderungan respons peserta terhadap pelaksanaan webinar dan workshop.

Data hasil pre-test dan post-test dianalisis secara deskriptif dengan menghitung persentase jawaban benar pada setiap butir soal. Perubahan hasil evaluasi ditunjukkan melalui perbandingan persentase jawaban benar sebelum dan setelah kegiatan. Data kuesioner juga dianalisis secara deskriptif melalui persentase respons peserta pada setiap aspek yang dinilai. Hasil analisis digunakan untuk menggambarkan perubahan pemahaman peserta dan tanggapan terhadap pelaksanaan kegiatan.

HASIL DAN PEMBAHASAN

Pelaksanaan Kegiatan

Kegiatan Kuliah Kerja Nyata (KKN) bertajuk "Digital Forensics: Recovery dan Analisis File Terhapus pada Media Penyimpanan Menggunakan Kali Linux untuk Investigasi Bukti Elektronik" dilaksanakan pada Sabtu, 4 Juli 2026, pukul 13.30–15.40 WIB melalui platform Zoom Meeting. Kegiatan ini diikuti oleh 20 peserta aktif dari total 34 pendaftar, yang berasal dari mahasiswa Universitas Muhammadiyah Jakarta, mitra kegiatan yaitu Himpunan Mahasiswa Informatika Universitas Komputer Indonesia (HMIF UNIKOM), serta perwakilan instansi lain seperti Universitas Nahdlatul Ulama Indonesia (UNUSIA), SMK Budhi Warman 1, dan masyarakat umum. Pemilihan webinar sebagai media utama penyampaian materi didasarkan pada kemampuannya menjangkau peserta dari berbagai latar belakang institusi tanpa terkendala jarak, sehingga penyebaran literasi digital forensics dapat berlangsung lebih luas (Adi, Gelar, & Masum, 2021).

Kegiatan webinar dan workshop dilaksanakan secara daring melalui platform Zoom Meeting dengan dihadiri oleh narasumber, panitia, serta peserta dari berbagai institusi, sebagaimana

ditunjukkan pada Gambar 1. Pelaksanaan secara daring ini memungkinkan peserta dari luar Universitas Muhammadiyah Jakarta, seperti perwakilan HMIF UNIKOM, UNUSIA, dan SMK Budhi Warman 1, serta Masyarakat umum untuk turut berpartisipasi secara langsung tanpa terkendala jarak dan lokasi.



Gambar 1. Dokumentasi Peserta Kegiatan melalui Zoom Meeting

Kegiatan kemudian dilakukan dengan sesi webinar dibuka dengan slide judul "Digital Forensics dan Data Recovery Menggunakan Kali Linux" sebagaimana ditunjukkan pada Gambar 2, yang secara visual merepresentasikan konsep investigasi digital melalui ilustrasi proses identifikasi bukti elektronik pada berbagai media penyimpanan menggunakan sistem operasi Kali Linux. Ilustrasi pada slide tersebut menggambarkan seorang investigator yang tengah memeriksa data digital menggunakan kaca pembesar, dikelilingi oleh berbagai media penyimpanan seperti hard disk, flashdisk, dan perangkat komputer, yang merepresentasikan cakupan objek investigasi dalam praktik digital forensics.



Gambar 2. Slide Pembuka Materi pada Sesi Webinar

Materi ini disampaikan oleh narasumber kepada seluruh peserta yang hadir melalui platform Zoom Meeting sebagai pengantar sebelum masuk ke pembahasan konsep dasar Digital Forensics secara lebih mendalam, mencakup pengertian bukti elektronik, mekanisme penghapusan file pada media penyimpanan, serta urgensi digital forensics dalam mendukung proses investigasi kejahatan siber. Penyampaian materi pengantar ini bertujuan untuk membangun kerangka berpikir awal bagi peserta sebelum mengikuti penjelasan yang lebih teknis mengenai prinsip kerja file recovery dan penggunaan tools forensik pada tahap berikutnya.

Setelah seminar selesai, kegiatan selanjutnya adalah sesi workshop berfokus demonstrasi langsung penggunaan sistem operasi Kali Linux yang dijalankan melalui Oracle VM VirtualBox, sebagaimana ditunjukkan pada Gambar 3. Pada sesi ini, narasumber mempraktikkan tahapan investigasi digital forensics menggunakan berkas image bukti elektronik berformat .E01 (*evidence_ss1.E01*), diawali dengan analisis struktur partisi dan sistem berkas menggunakan perintah *mmls* untuk mengidentifikasi offset sektor serta jenis partisi yang tersedia pada media penyimpanan. Selanjutnya, narasumber melakukan proses recovery file menggunakan perintah *tsk_recover* dari

perangkat lunak The Sleuth Kit (TSK), yang berhasil memulihkan sejumlah file dari partisi FAT32 ke dalam direktori hasil pemulihan (*recover2*).

Seluruh berkas yang menjadi target pemulihan pada demonstrasi tersebut berhasil dipulihkan sepenuhnya dari partisi FAT32, meskipun dokumentasi rinci berupa jumlah spesifik per jenis file serta nilai hash sebelum dan sesudah proses recovery tidak dicatat secara sistematis selama kegiatan berlangsung. Dari sisi forensic soundness, seluruh proses analisis dilakukan terhadap salinan berkas image bukti (*evidence_ss1.E01*) yang dijalankan pada lingkungan virtual (Oracle VM VirtualBox) sehingga media sumber tidak mengalami perubahan langsung, namun langkah verifikasi integritas berupa perbandingan nilai hash serta pencatatan chain of custody secara formal belum diterapkan dalam kegiatan ini. Aspek tersebut menjadi catatan perbaikan penting bagi pelaksanaan kegiatan serupa di masa mendatang.



Gambar 3. Praktik Recovery File pada Sesi Workshop

Melalui demonstrasi tersebut, peserta dapat mengamati secara langsung alur kerja investigasi bukti elektronik, mulai dari identifikasi struktur media penyimpanan, penentuan sistem berkas, hingga proses ekstraksi file yang telah terhapus. Pendekatan praktik berbasis command-line ini memberikan pemahaman konkret kepada peserta mengenai cara kerja tools forensik di balik proses recovery, sekaligus memperlihatkan bahwa keberhasilan pemulihan data sangat bergantung pada ketepatan identifikasi sistem berkas sebelum dilakukan ekstraksi (Brunty, 2023).

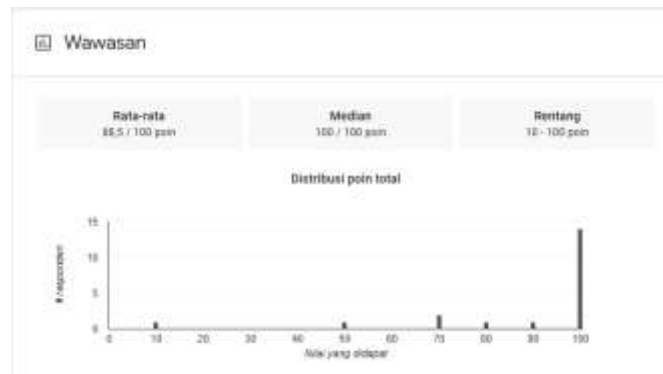
Evaluasi Kegiatan

Evaluasi kegiatan dilakukan untuk mengukur tingkat pemahaman peserta terhadap materi yang telah disampaikan selama sesi webinar dan workshop, sekaligus untuk menilai efektivitas pelaksanaan program secara keseluruhan. Instrumen evaluasi yang digunakan berupa pre-test dan post-test yang dibagikan melalui Google Forms, masing-masing terdiri atas sepuluh pertanyaan yang mencakup konsep dasar Digital Forensics, karakteristik media penyimpanan data, mekanisme yang terjadi saat file dihapus, prinsip kerja file recovery, perbedaan antara data recovery dan data carving, hingga pengenalan tools serta keunggulan sistem operasi Kali Linux dalam mendukung proses investigasi bukti elektronik.

Instrumen pre-test dan post-test tersebut disusun langsung oleh tim pelaksana berdasarkan materi yang akan disampaikan, tanpa melalui tahapan uji validitas dan reliabilitas secara formal maupun penyusunan kisi-kisi soal yang terstruktur. Keterbatasan ini perlu menjadi perhatian dalam menginterpretasikan hasil evaluasi, mengingat kualitas psikometrik instrumen turut memengaruhi akurasi pengukuran perubahan pemahaman peserta.

Pre-test diberikan kepada peserta sebelum sesi webinar dimulai dengan tujuan untuk mengidentifikasi tingkat pemahaman awal mereka mengenai Digital Forensics dan keamanan sistem informasi, sekaligus menjadi baseline untuk mengukur peningkatan pemahaman setelah mengikuti rangkaian kegiatan. Pengisian pre-test dilakukan secara mandiri oleh peserta pada tahap pembukaan acara, sebelum narasumber menyampaikan materi konseptual pada sesi webinar. Melalui evaluasi awal ini, tim KKN dapat memperoleh gambaran mengenai sejauh mana peserta telah memiliki bekal pengetahuan sebelum mengikuti pelatihan, sekaligus menjadi acuan untuk

menilai kontribusi kegiatan terhadap peningkatan literasi digital forensics peserta. Hasil rekapitulasi skor pre-test secara keseluruhan ditampilkan pada Gambar 4.



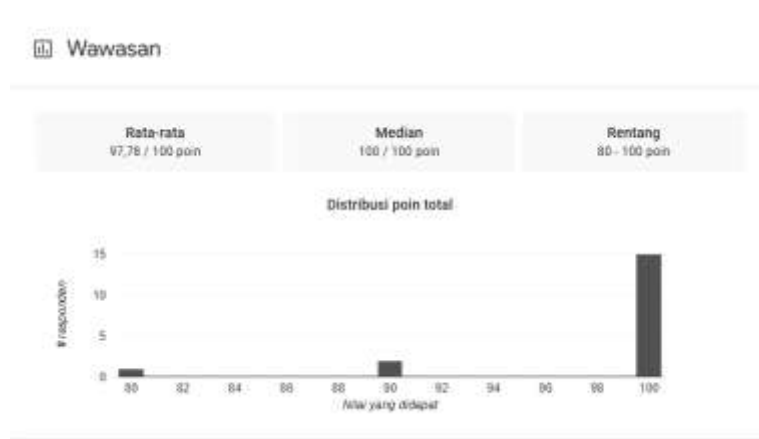
Gambar 4. Distribusi Skor Total Pre-Test Peserta

Hasil pre-test menunjukkan bahwa peserta memperoleh skor rata-rata 88,5 dari 100 poin, dengan nilai median mencapai 100 poin dan rentang skor antara 10 hingga 100 poin, sebagaimana ditunjukkan pada Gambar 4. Mayoritas peserta, yaitu sebanyak 14 dari 20 responden, telah menjawab seluruh pertanyaan dengan benar dan memperoleh skor sempurna (100 poin), sementara beberapa peserta lainnya memperoleh skor yang lebih rendah pada rentang 50 hingga 90 poin, bahkan terdapat satu peserta yang hanya memperoleh 10 poin. Distribusi skor tersebut mengindikasikan bahwa meskipun sebagian besar peserta telah memiliki pemahaman awal yang baik mengenai konsep Digital Forensics dan penggunaan Kali Linux, masih terdapat kesenjangan pemahaman pada sebagian kecil peserta yang perlu diperkuat melalui sesi webinar dan workshop.

Kondisi ini turut mengindikasikan adanya ceiling effect pada instrumen pre-test, di mana proporsi besar peserta yang telah mencapai skor maksimum sejak awal membatasi kemampuan instrumen untuk mendeteksi peningkatan pemahaman pada kelompok tersebut, sehingga peningkatan yang teramati pada post-test lebih merepresentasikan perbaikan pemahaman peserta dengan skor awal rendah dibandingkan seluruh peserta secara umum.

Setelah mengikuti seluruh rangkaian sesi webinar dan workshop, peserta kembali diminta untuk mengisi post-test dengan instrumen pertanyaan yang sama seperti pre-test. Post-test ini bertujuan untuk mengukur peningkatan pemahaman peserta setelah memperoleh materi konseptual maupun pengalaman praktik langsung menggunakan Kali Linux.

Penggunaan butir soal yang identik antara pre-test dan post-test berpotensi menimbulkan testing effect, yaitu peningkatan skor yang sebagian disebabkan oleh familiaritas peserta terhadap soal yang sama, bukan semata-mata karena peningkatan pemahaman substantif. Idealnya, evaluasi semacam ini menggunakan bank soal yang setara namun tidak identik untuk meminimalkan bias tersebut.



Gambar 5. Distribusi Skor Total Post-Test Peserta

Hasil post-test menunjukkan peningkatan yang cukup besar, dengan skor rata-rata naik menjadi 97,78 dari 100 poin, nilai median tetap berada di 100 poin, dan rentang skor menyempit menjadi 80 hingga 100 poin, sebagaimana ditunjukkan pada Gambar 5. Mayoritas peserta, yaitu sebanyak 15 dari 20 responden, berhasil memperoleh skor sempurna (100 poin), sementara sisanya memperoleh skor pada rentang 80 hingga 90 poin. Dibandingkan dengan hasil pre-test yang sebelumnya memiliki rentang skor 10 hingga 100 poin, penyempitan rentang pada post-test ini mengindikasikan bahwa kesenjangan pemahaman antarpeserta berhasil diperkecil, dan hampir seluruh peserta telah mencapai tingkat pemahaman yang seragam dan tinggi mengenai Digital Forensics setelah mengikuti kegiatan.

Perlu dicatat bahwa rekapitulasi data mentah per-peserta untuk post-test sudah tidak dapat ditelusuri kembali oleh tim pelaksana pada saat penyusunan artikel ini, sehingga verifikasi independen terhadap konsistensi rerata yang dilaporkan tidak dapat dilakukan. Angka rerata 97,78 yang disajikan perlu dibaca dengan kehati-hatian, dan tim merekomendasikan agar kegiatan pengabdian serupa di masa mendatang menyimpan data evaluasi mentah secara lebih tertata untuk memungkinkan audit dan analisis lanjutan.

Untuk mengetahui besarnya peningkatan pemahaman peserta setelah mengikuti kegiatan, dilakukan analisis menggunakan metode *Normalized Gain* (N-Gain) dengan membandingkan skor rata-rata pre-test dan post-test. Rumus perhitungan N-Gain yang digunakan adalah sebagai berikut:

Perhitungan N-Gain pada kegiatan ini dilakukan berdasarkan skor rata-rata kelompok, bukan dihitung secara individual per peserta kemudian dirangkum distribusinya. Pendekatan berbasis rerata kelompok ini memiliki keterbatasan dibandingkan analisis N-Gain per peserta atau uji statistik berpasangan seperti uji Wilcoxon, yang lebih sesuai untuk desain evaluasi pre-test-post-test pada subjek yang sama.

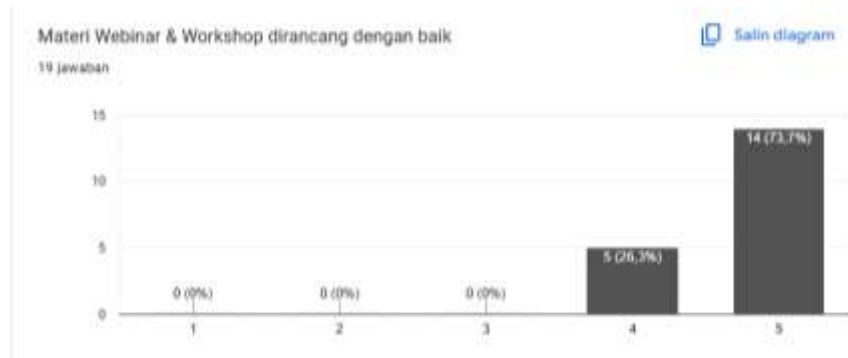
$$N\text{-Gain} = (Post\text{-Test} - Pre\text{-Test}) / (Skor\ Maks - Pre\text{-Test}) = (97,78 - 88,5) / (100 - 88,5) = 0,81$$

Hasil perhitungan menunjukkan nilai N-Gain sebesar 0,81, yang berada pada kategori tinggi ($g \geq 0,7$) (Hake, 1998). Nilai ini menunjukkan bahwa kombinasi penyampaian materi konseptual pada sesi webinar dengan praktik langsung pada sesi workshop efektif dalam meningkatkan pemahaman peserta mengenai Digital Forensics dan penggunaan Kali Linux untuk investigasi bukti elektronik. Selain itu, penyempitan rentang skor dari 10–100 pada pre-test menjadi 80–100 pada post-test turut memperkuat indikasi bahwa kegiatan ini tidak hanya meningkatkan skor rata-rata secara umum, tetapi juga berhasil mengangkat pemahaman peserta yang sebelumnya berada pada level terendah, sehingga kesenjangan pemahaman antarpeserta dapat diperkecil secara signifikan.

Nilai N-Gain tersebut menggambarkan besaran peningkatan skor secara deskriptif dan bukan merupakan bukti signifikansi statistik, mengingat penafsirannya perlu mempertimbangkan ceiling effect yang telah teridentifikasi pada skor pre-test serta keterbatasan pendekatan N-Gain berbasis rerata kelompok yang telah diuraikan sebelumnya.

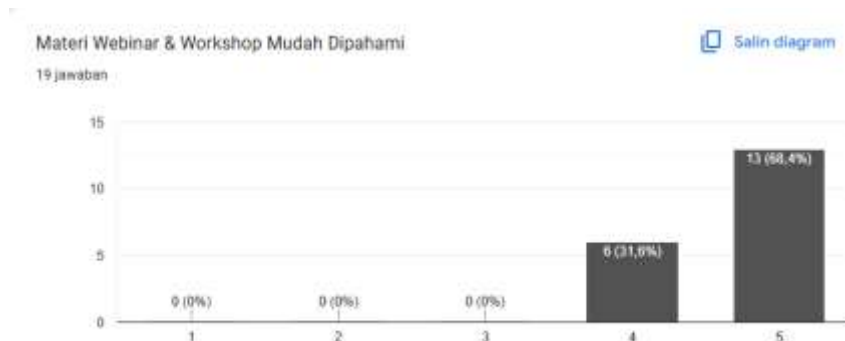
Selain evaluasi kognitif melalui pre-test dan post-test, penilaian terhadap kualitas pelaksanaan kegiatan juga dilakukan melalui kuesioner umpan balik yang diisi oleh 19 peserta menggunakan skala Likert 1 hingga 5, dengan skala 1 menyatakan "Sangat Tidak Setuju" dan skala 5 menyatakan "Sangat Setuju". Kuesioner ini mencakup penilaian terhadap perancangan materi, kemudahan pemahaman, serta wawasan yang diperoleh peserta selama mengikuti webinar dan workshop.

Response rate kuesioner kepuasan tercatat sebesar 95% (19 dari 20 peserta aktif), tanpa informasi yang jelas mengenai alasan satu peserta tidak mengisi kuesioner tersebut. Perlu ditegaskan pula bahwa hasil kepuasan peserta ini menggambarkan persepsi terhadap kualitas pelaksanaan kegiatan, dan tidak dapat dijadikan bukti langsung atas peningkatan kompetensi teknis peserta.



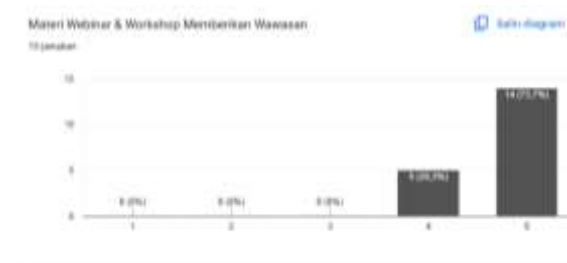
Gambar 6. Penilaian Peserta terhadap Perancangan Materi Webinar & Workshop

Pada aspek perancangan materi, sebanyak 14 dari 19 peserta (73,7%) menyatakan "Sangat Setuju" bahwa materi webinar dan workshop dirancang dengan baik, sedangkan 5 peserta (26,3%) lainnya menyatakan "Setuju", sebagaimana ditunjukkan pada Gambar 6. Tidak terdapat peserta yang memberikan penilaian negatif (skala 1 hingga 3), yang menunjukkan bahwa struktur dan penyusunan materi kegiatan telah sesuai dengan kebutuhan dan ekspektasi peserta.



Gambar 7. Penilaian Peserta terhadap Kemudahan Pemahaman Materi

Pada aspek kemudahan pemahaman, sebanyak 13 peserta (68,4%) menyatakan "Sangat Setuju" bahwa materi webinar dan workshop mudah dipahami, sedangkan 6 peserta (31,6%) menyatakan "Setuju", sebagaimana ditunjukkan pada Gambar 7. Hasil ini konsisten dengan temuan pada evaluasi pre-test dan post-test, di mana peningkatan skor N-Gain sebesar 0,81 turut mengindikasikan bahwa penyampaian materi secara interaktif berhasil disajikan dengan cara yang mudah dicerna oleh peserta dari berbagai latar belakang institusi.



Gambar 8. Penilaian Peserta terhadap Wawasan yang Diperoleh

Pada aspek wawasan yang diperoleh, sebanyak 14 peserta (73,7%) menyatakan "Sangat Setuju" bahwa materi webinar dan workshop memberikan wawasan baru, sedangkan 5 peserta (26,3%) menyatakan "Setuju", sebagaimana ditunjukkan pada Gambar 8. Secara keseluruhan, hasil ketiga aspek penilaian ini menunjukkan respons yang sangat positif dari peserta, dengan seluruh jawaban terkonsentrasi pada skala 4 dan 5, tanpa adanya penilaian negatif sama sekali terhadap kualitas perancangan, kemudahan pemahaman, maupun wawasan yang diperoleh dari kegiatan.

Berdasarkan keseluruhan hasil evaluasi yang telah dipaparkan, baik melalui pre-test dan post-test maupun kuesioner umpan balik, dapat disimpulkan bahwa kegiatan webinar dan workshop "Digital Forensics dan Data Recovery Menggunakan Kali Linux" berhasil mencapai tujuan pembelajaran yang telah ditetapkan. Peningkatan skor rata-rata dari 88,5 menjadi 97,78 poin dengan kategori N-Gain tinggi (0,81) menunjukkan bahwa peserta mengalami peningkatan pemahaman yang signifikan setelah mengikuti kegiatan, sementara hasil kuesioner umpan balik yang didominasi penilaian "Sangat Setuju" pada seluruh aspek materi webinar dan workshop turut mengonfirmasi bahwa peningkatan tersebut sejalan dengan tingkat kepuasan peserta terhadap kualitas penyampaian materi. Dengan demikian, evaluasi kognitif dan evaluasi kepuasan peserta saling melengkapi dalam menggambarkan keberhasilan kegiatan ini secara menyeluruh.

Pembahasan

Peningkatan skor rata-rata dari 88,5 pada pre-test menjadi 97,78 pada post-test, dengan nilai N-Gain sebesar 0,81 (kategori tinggi), menunjukkan bahwa kombinasi penyampaian materi konseptual pada sesi webinar dengan praktik langsung pada sesi workshop efektif dalam memperkuat pemahaman peserta mengenai Digital Forensics. Penyempitan rentang skor dari 10–100 pada pre-test menjadi 80–100 pada post-test juga mengindikasikan bahwa kegiatan ini tidak hanya meningkatkan capaian rata-rata, tetapi juga berhasil mengangkat pemahaman peserta yang sebelumnya berada pada level terendah. Temuan ini sejalan dengan hasil pelatihan pengenalan dan instalasi Kali Linux bagi mahasiswa, yang menunjukkan bahwa pemaparan konsep keamanan sistem informasi disertai praktik langsung dapat meningkatkan kesiapan generasi muda dalam menghadapi ancaman kejahatan siber (Syahib, Yasin, & Rauf, 2023).

Demonstrasi penggunaan Kali Linux melalui Oracle VM VirtualBox pada sesi workshop, mulai dari analisis struktur partisi menggunakan *mmfs* hingga proses recovery file menggunakan *tsk_recover*, memberikan pengalaman konkret kepada peserta mengenai alur kerja investigasi bukti elektronik yang tidak dapat diperoleh hanya melalui pemaparan teori. Pendekatan ini memperkuat pandangan bahwa keandalan hasil recovery sangat bergantung pada pemahaman investigator terhadap validitas dan cara kerja tools forensik yang digunakan, sehingga praktik langsung menjadi bagian penting dari pembelajaran digital forensics yang bertanggung jawab (Brunty, 2023).

Hasil kuesioner umpan balik untuk kategori Feedback Webinar & Workshop menunjukkan respons yang sangat positif, dengan mayoritas peserta menyatakan "Sangat Setuju" pada aspek perancangan materi (73,7%), kemudahan pemahaman (68,4%), dan wawasan yang diperoleh (73,7%), tanpa ada satu pun penilaian negatif. Konsistensi antara tingginya nilai N-Gain dan tingginya tingkat kepuasan peserta memperlihatkan bahwa peningkatan pemahaman yang terukur secara kuantitatif juga dirasakan secara langsung oleh peserta sebagai pengalaman belajar yang bermakna, bukan sekadar capaian angka pada instrumen evaluasi.

Sebagaimana diuraikan pada bagian permasalahan mitra, HMIF UNIKOM menghadapi keterbatasan akses terhadap pelatihan berbasis praktik langsung serta minimnya pengalaman anggota dalam mengoperasikan perangkat forensik digital secara langsung, mengingat materi tersebut belum menjadi bagian dari kurikulum yang mereka tempuh. Hasil evaluasi yang menunjukkan peningkatan pemahaman signifikan mengindikasikan bahwa pengenalan tools open source pada Kali Linux mampu menjadi solusi yang relevan dan aplikatif bagi mitra, sekaligus membuktikan bahwa kompetensi digital forensics dapat dibangun melalui perangkat lunak open source yang mudah diakses tanpa bergantung pada perangkat lunak komersial (Al-Dhaqm, Ikuesan, Kebande, Razak, Grispos, & Choo, 2021).

Partisipasi peserta dari berbagai institusi, yaitu UMJ, HMIF UNIKOM, UNUSIA, SMK Budhi Warman 1, Serta Masyarakat umum yang difasilitasi melalui pelaksanaan secara daring, memperluas jangkauan penyebaran literasi digital forensics melampaui satu institusi saja. Pemilihan webinar sebagai media utama terbukti mendukung keberhasilan ini, karena mampu menjangkau peserta secara lebih luas tanpa terkendala jarak (Adi, Gelar, & Masum, 2021), sementara tantangan teknik anti-forensics yang terus berkembang seperti secure wipe dan enkripsi data menegaskan pentingnya keberlanjutan pelatihan serupa di masa mendatang agar kompetensi peserta tetap relevan dengan perkembangan ancaman keamanan siber (Yaacoub, Noura, Salman, & Chehab, 2021).

Secara keseluruhan, kelima temuan tersebut memperlihatkan bahwa kegiatan webinar dan workshop ini tidak hanya berhasil meningkatkan pemahaman kognitif peserta secara terukur, tetapi juga menjawab kebutuhan riil mitra akan pelatihan digital forensics yang aplikatif, ekonomis, dan dapat diakses secara kolaboratif lintas institusi, sehingga dapat dijadikan model pengabdian masyarakat yang efektif untuk penguatan literasi keamanan siber (Sakti, 2025).

Keterbatasan Kegiatan

Kegiatan pengabdian ini memiliki sejumlah keterbatasan yang perlu menjadi perhatian dalam menginterpretasikan hasil maupun dalam replikasi pada kegiatan serupa. Pertama, instrumen evaluasi belum melalui uji validitas dan reliabilitas formal. Kedua, penggunaan soal yang identik pada pre-test dan post-test berpotensi menimbulkan testing effect, sementara skor pre-test yang sudah tinggi sejak awal menyebabkan ceiling effect yang membatasi sensitivitas pengukuran. Ketiga, dokumentasi teknis berupa data performa recovery (jumlah file, tipe file, dan nilai hash) serta langkah verifikasi forensic soundness belum dicatat secara sistematis. Keempat, evaluasi hanya dilakukan pada satu titik waktu tanpa monitoring lanjutan (follow-up) terhadap retensi pemahaman maupun penerapan keterampilan peserta pascakegiatan, sehingga klaim keberhasilan kegiatan sebagai model pelatihan yang dapat direplikasi perlu dimaknai sebagai indikasi awal, bukan kesimpulan definitif. Kegiatan pengabdian masyarakat berikutnya disarankan menerapkan monitoring pascapelatihan serta pencatatan data yang lebih tertata untuk memperkuat validitas temuan.

KESIMPULAN

Kegiatan Kuliah Kerja Nyata (KKN) "Digital Forensics: Recovery dan Analisis File Terhapus pada Media Penyimpanan Menggunakan Kali Linux untuk Investigasi Bukti Elektronik" yang diselenggarakan bersama mitra Himpunan Mahasiswa Informatika Universitas Komputer Indonesia (HMIF UNIKOM) berhasil mencapai tujuan yang telah ditetapkan, yaitu meningkatkan pemahaman peserta mengenai konsep dasar Digital Forensics sekaligus membekali keterampilan praktis dalam melakukan recovery dan analisis file terhapus menggunakan sistem operasi Kali Linux. Keberhasilan ini terlihat dari peningkatan skor rata-rata evaluasi dari 88,5 pada pre-test menjadi 97,78 pada post-test, dengan nilai N-Gain sebesar 0,81 yang tergolong kategori tinggi, serta penyempitan rentang skor peserta yang menunjukkan berkurangnya kesenjangan pemahaman antarpeserta setelah mengikuti kegiatan.

Perlu ditegaskan bahwa data yang tersedia dalam kegiatan ini terutama mendukung peningkatan pemahaman kognitif dan persepsi kepuasan peserta, sedangkan bukti kompetensi keterampilan praktis

dalam melakukan recovery dan analisis file terhapus secara mandiri dan berkelanjutan belum dapat dipastikan tanpa data performa praktik maupun observasi keterampilan pascakegiatan.

Hasil kuesioner umpan balik untuk kategori Feedback Webinar & Workshop turut memperkuat capaian tersebut, dengan mayoritas peserta menyatakan "Sangat Setuju" terhadap perancangan materi, kemudahan pemahaman, dan wawasan yang diperoleh, tanpa adanya penilaian negatif sama sekali. Konsistensi antara peningkatan pemahaman kognitif dan tingkat kepuasan peserta menunjukkan bahwa pendekatan yang mengombinasikan penyampaian materi konseptual pada sesi webinar dengan praktik langsung menggunakan tools open source seperti The Sleuth Kit pada sesi workshop merupakan model pelatihan yang efektif untuk membangun kompetensi digital forensics secara aplikatif dan ekonomis.

Dengan demikian, pendekatan pelatihan berbasis webinar dan workshop daring ini dapat dijadikan model pengabdian masyarakat yang berkelanjutan untuk penguatan literasi keamanan siber, khususnya dalam menghadapi tantangan investigasi bukti elektronik yang terus berkembang seiring munculnya teknik anti-forensics di era digital.

REFERENSI

- Adi, P., Gelar, G. R., & Masum, A. N. (2021). Pemanfaatan webinar sebagai alternatif digitalisasi informasi dalam seminar kurikulum. *Indonesian Journal of Digital Business*, 1(1), 43–49.
- Al-Dhaqm, A., Ikuesan, R. A., Kebande, V. R., Razak, S. A., Grispos, G., & Choo, K.-K. R. (2021). Digital forensics subdomains: The state of the art and future directions. *IEEE Access*, 9, 152476–152502. <https://doi.org/10.1109/ACCESS.2021.3124262>
- Brunty, J. (2023). Validation of forensic tools and methods: A primer for the digital forensics examiner. *WIREs Forensic Science*, 5(2), e1474. <https://doi.org/10.1002/wfs2.1474>
- Hake, R. R. (1998). Interactive-engagement versus traditional methods: A six-thousand-student survey of mechanics test data for introductory physics courses. *American Journal of Physics*, 66(1), 64–74.
- Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges and future directions. *IEEE Access*, 10, 11065–11089. <https://doi.org/10.1109/ACCESS.2022.3142508>
- Kusuma, A. W., Alwi, E. I., & Ramdaniah, R. (2024). Analisis bukti digital pada media penyimpanan flash disk menggunakan metode National Institute of Standards and Technology (NIST). *Cyber Security dan Forensik Digital*, 7(1), 18–24. <https://doi.org/10.14421/csecurity.2024.7.1.4345>
- Offensive Security. (2023). *Kali Linux documentation*. <https://www.kali.org/docs/>
- Sakti, A. (2025). Pengaruh pendidikan dan pelatihan digital forensik terhadap kualitas penanganan kasus kejahatan siber. *Populer: Jurnal Penelitian Mahasiswa*, 4(1), 104–109. <https://doi.org/10.58192/populer.v4i1.2974>
- Santoshi, D., Pulgam, N., & Mane, V. (2022). Analysis and simulation of Kali Linux digital forensic tools. *Proceedings of the 7th International Conference on Innovations and Research in Technology and Engineering (ICIRTE-2022)*. <https://doi.org/10.2139/ssrn.4111750>
- Sugiyono. (2022). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Alfabeta.
- Susanti, L. (2025). Analisis efektivitas file carving dalam forensik digital pada flashdisk dengan tools Autopsy dan FTK Imager. *Jurnal Locus: Penelitian & Pengabdian*, 4(9), 8978–8989.
- Syahib, M. I., Yasin, M. A., & Rauf, B. W. (2023). Pengenalan dan instalasi Kali Linux untuk langkah awal pengetahuan tentang keamanan sistem informasi. *ANO A: Jurnal Pengabdian Masyarakat Fakultas Teknik*, 1(02), 32–38. <https://doi.org/10.51454/anoa.v1i02.275>
- Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Digital forensics vs. anti-digital forensics: Techniques, limitations and recommendations. *arXiv preprint*, arXiv:2103.17028. <https://arxiv.org/abs/2103.17028>