|  |  |  |  |
| --- | --- | --- | --- |
| binadarmalogo.png | **RENCANA PEMBELAJARAN SEMESTER *(SEMESTER LESSON PLAN)*** | Nomor Dok | FRM/KUL/01/02 |
| Nomor Revisi | 02 |
| Tgl. Berlaku | 1 Januari 2018 |
| Klausa ISO | 7.5.1 & 7.5.5 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Disusun oleh** *(Prepared by)* | **Diperiksa oleh** *(Checked by)* | **Disetujui oleh** *(Approved by)* | **Tanggal Validasi**  *(Valid date)* |
|  |  |  |  |
|  |  |  |

1. Fakultas *(Faculty)* : Ilmu Komputer
2. Program Studi *(Study Program)*  : Magister Teknik Informatika Jenjang *(Grade)* : S-2
3. Mata Kuliah *(Course)* : Computer and Network Forensic SKS *(Credit) : 3* Semester *(Semester)* :  *1*
4. Kode Mata Kuliah *(Code)* : MTIK-316 Sertifikasi *(Certification)* : Ya *(Yes)* Tidak *(No)*
5. Mata Kuliah Prasyarat *(Prerequisite)*  :  - ..............................................
6. Dosen Koordinator *(Coordinator)* : -

✓

1. Dosen Pengampuh *(Lecturer)* :  Tim *(Team)* Mandiri *(Personal)*
2. Capaian Pembelajaran Mata Kuliah (*Course* *Learning Outcomes*) :

|  |  |  |
| --- | --- | --- |
| Capaian Pembelajaran Lulusan Program Studi MTI (CPL) | Sikap  Pengetahuan  Keterampilan Umum  Keterampilan Khusus | 1. Bertakwa kepada Tuhan Yang Maha Esa dan mampu menunjukkan sikap religius 2. Menjunjung tinggi nilai kemanusiaan dalam menjalankan tugas berdasarkan agama, moral dan etika. 3. Dapat berperan sebagai warga negara yang bangga dan cinta tanah air, memiliki nasionalisme serta rasa tanggungjawab pada negara dan bangsa. 4. Dapat berkontribusi dalam peningkatan mutu kehidupan bermasyarakat, berbangsa, dan bernegara berdasarkan Pancasila. 5. Dapat bekerja sama dan memiliki kepekaan sosial serta kepedulian terhadap masyarakat dan lingkungan. 6. Dapat menghargai keanekaragaman budaya, pandangan, agama, dan kepercayaan, serta pendapat atau temuan orisinal orang lain. 7. Taat hukum dan disiplin dalam kehidupan bermasyarakat dan bernegara. 8. Menunjukkan sikap bertanggungjawab atas pekerjaan di bidang keahliannya secara mandiri. 9. Menginternalisasi nilai, norma, dan etika akademik. 10. Menginternalisasi semangat kemandirian, kejuangan, dan kewirausahaan 11. Memiliki kemampuan memecahkan permasalahan sains dan teknologi dalam bidang Ilmu Komputer/Informatika melalui pendekatan inter atau multidisipliner. 12. Mempunyai pengetahuan dan pemahaman sejumlah tema ilmu komputer, termasuk abstraksi, kompleksitas dan evolusi dari perubahan/pengembangan keilmuan dan prinsip-prinsip umum ilmu komputer seperti berbagi (*sharing*) sumber daya, keamanan (*security*) dan bekerja secara paralel (*concurrency*). 13. Memiliki pengetahuan sesuai dengan capaian pembelajaran program studi S2 Ilmu Komputer pada ***“Domain Spesific”*** atau ***“Research”*** sesuai dengan konsentrasi Program Studi yaitu *Enterprise IT Infrastructure, Enterprise Network Security,* dan *Enterprise Software Engineering.* 14. Mampu mengembangkan pemikiran logis, kritis, sistematis, dan kreatif melalui penelitian ilmiah, penciptaan desain atau karya seni dalam bidang ilmu pengetahuan dan teknologi yang memperhatikan dan menerapkan nilai humaniora sesuai dengan bidang keahliannya, menyusun konsepsi ilmiah dan hasil kajiannya berdasarkan kaidah, tata cara, dan etika ilmiah dalam bentuk tesis, dan memublikasikan tulisan dalam jurnal ilmiah terakreditasi tingkat nasional dan mendapatkan pengakuan internasional berbentuk presentasi ilmiah atau yang setara; 15. Mampu melakukan validasi akademik atau kajian sesuai bidang keahliannya dalam menyelesaikan masalah di masyarakat atau industri yang relevan melalui pengembangan pengetahuan dan keahliannya. 16. Mampu menyusun ide, hasil pemikiran, dan argumen saintifik secara bertanggung jawab dan berdasarkan etika akademik, serta mengkomunikasikannya melalui media kepada masyarakat akademik dan masyarakat luas. 17. Mampu mengidentifikasi bidang keilmuan yang menjadi obyek penelitiannya dan memposisikan ke dalam suatu peta penelitian yang dikembangkan melalui pendekatan interdisiplin atau multidisiplin. 18. Mampu mengambil keputusan dalam konteks menyelesaikan masalah pengembangan ilmu pengetahuan dan teknologi yang memperhatikan dan menerapkan nilai humaniora berdasarkan kajian analisis atau eksperimental terhadap informasi dan data. 19. Mampu mengelola, mengembangkan dan memelihara jaringan kerja dengan kolega, sejawat di dalam lembaga dan komunitas penelitian yang lebih luas. 20. Mampu meningkatkan kapasitas pembelajaran secara mandiri; dan 21. Mampu mendokumentasikan, menyimpan, mengamankan, dan menemukan kembali data hasil penelitian dalam rangka menjamin kesahihan dan mencegah plagiasi.   Mampu mendesain, menganalisis, dan mengimplementasikan *behaviour* sistem berbasis komputer yang berkualitas (terukur dan teruji) dengan mengaplikasikannya pada *domain* yang sesuai dengan konsentrasi Program Studi yaitu *Enterprise IT Infrastructure, Enterprise Network Security*, dan *Enterprise Software Engineering* berdasarkan kebutuhan dan keterbatasan sistem, serta mampu mengelolanya dengan tepat. |
| Capaian Pembelajaran Mata Kuliah (CPMK) | Mampu mendesain, menganalisis dan mengevaluasi prinsip-prinsip tingkat lanjut mengenai keterampilan konkret dalam memahami proses investigasi forensik komputer dan jaringan, yang meliputi pemahaman akan kejahatan dan acaman siber, pembacaan dan analisis log, otentikasi, anslisi forensik *file system* yang bertujuan untuk penegakan hukum atau meningkatkan layanan keamanan dalam suatu organisasi. | |

1. Deskripsi Mata Kuliah

|  |  |
| --- | --- |
| Deskripsi Singkat Mata Kuliah | Merupakan mata kuliah khusus pada konsentrasi Program Studi yaitu “*Enterprise Network Security”* yang memberikan gambaran mendesain, menganalisis dan mengevaluasi prinsip-prinsip tingkat lanjut mengenai keterampilan konkret dalam memahami proses investigasi forensik komputer dan jaringan, yang meliputi pemahaman akan kejahatan dan acaman siber, pembacaan dan analisis log, otentikasi, anslisi forensik *file system* yang bertujuan untuk penegakan hukum atau meningkatkan layanan keamanan dalam suatu organisasi. |

1. Bahan Kajian

|  |  |
| --- | --- |
| Bahan Kajian (Materi Pembelajaran) | 1. *Cyber Crime and computer crime* 2. *Hacking and cracking* 3. *Credit card and ATM frauds* 4. *Computer Forensics* 5. *Host-Based Forensics* 6. *Law enforcement applications include* 7. *Capturing logs* 8. *Advanced Host-Based Forensic Analysis* 9. *Email Tracking* 10. *IP Tracking* 11. *Network Forensics* 12. *Advanced Network Analysis* 13. *Event Reconstruction and Correlation* |

1. Implementasi Pembelajaran Mingguan *(Implementation Process of weekly learning time)*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Minggu** | **Sub CPMK**  **(Kemampuan akhir yang direncanakan)** | **Bahan Kajian/Materi Pembelajaran**  *(Study Material)* | **Bentuk dan Metode Pembelajaran**  *(Learning Method)* | **Sumber Belajar**  *(Learning Resource)* | **Penilaian** | | |
| **Indikator**  *(Indicator)* | **Kriteria & bentuk** | **Bobot** |
| 1 | Mampu menganalisa dan mengevaluasi mengenai prinsip  konsep digital forensik, jenis-jenis kejahatan dunia maya dan aplikasi komputer forensik Bagian 1  (CPMK 1.1) | 1. *Cyber Crime and computer crime* 2. *Hacking and cracking* 3. *Credit card and ATM frauds* | Kuliah dan Diskusi *(Discovery Learning, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisa dan mengevaluasi mengenai prinsip  konsep digital forensik, jenis-jenis kejahatan dunia maya dan aplikasi komputer forensik Bagian 1 | **Kriteria :** Ketepatan dalam menganalisa dan mengevaluasi mengenai prinsip  konsep digital forensik, jenis-jenis kejahatan dunia maya dan aplikasi komputer forensik Bagian 1  **Bentuk :**  Diskusi |  |
| 2 | Mampu menganalisa dan mengevaluasi mengenai prinsip  konsep digital forensik, jenis-jenis kejahatan dunia maya dan aplikasi komputer forensik Bagian 2  (CPMK 1.2) | 1. *Web technology* 2. *Cryptography* 3. *Emerging digital crimes and modules* | Kuliah, Tugas dan Diskusi *(Discovery Learning, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisa dan mengevaluasi mengenai prinsip  konsep digital forensik, jenis-jenis kejahatan dunia maya dan aplikasi komputer forensik Bagian 2 | **Kriteria :** Ketepatan dalam menganalisa dan mengevaluasi mengenai prinsip  konsep digital forensik, jenis-jenis kejahatan dunia maya dan aplikasi komputer forensik Bagian 2  **Bentuk :**  Diskusi |  |
| 3 | Mampu menganalisis dan mengevaluasi aturan layanan pada proses akuisisi dan otentikasi komputer forensik Bagian 1 (CPMK 1.3) | 1. *Definition and Cardinal Rules* 2. *Data Acquisition and Authentication Process* 3. *Windows Systems-FAT12, FAT16, FAT32 and NTFS* 4. *UNIX file Systems* 5. *MAC file systems* | Kuliah, Tugas dan Diskusi *(Discovery Learning, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisis dan mengevaluasi aturan pada proses akuisisi dan otentikasi komputer forensik Bagian 1 | **Kriteria :** Ketepatan dalam menganalisis dan mengevaluasi aturan pada proses akuisisi dan otentikasi komputer forensik Bagian 1  **Bentuk :**  Diskusi |  |
| 4 | Kuis 1 | | | | | | 10% |  | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] |
| 5 | Mampu menganalisis dan mengevaluasi aturan layanan pada proses akuisisi dan otentikasi komputer forensik Bagian 2 (CPMK 1.4) | 1. *Computer artifacts* 2. *Internet Artifacts* 3. *OS Artifacts* 4. *Forensic applications* | Kuliah, Tugas dan Diskusi *(Discovery Learning, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisis dan mengevaluasi aturan layanan pada proses akuisisi dan otentikasi komputer forensik Bagian 2 | **Kriteria :** Ketepatan dalam menganalisis dan mengevaluasi aturan layanan pada proses akuisisi dan otentikasi komputer forensik Bagian 2  **Bentuk :**  Diskusi |  |
| 6 | Mampu menganalisis dan mengevaluasi forensik berbasis *Host* Bagian 1 (CPMK 1.5) | 1. *Planning for conducting an investigation* 2. *Determining what evidence is needed* 3. *Acquiring evidence by preserving and protecting evidence and keeping it clean and secure* | Kuliah, Tugas dan Diskusi *(Discovery Learning, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisis dan mengevaluasi forensik berbasis *Host* Bagian 1 ( | **Kriteria :** Ketepatan dalam menganalisis dan mengevaluasi forensik berbasis *Host* Bagian 1  **Bentuk :**  Diskusi |  |
| 7 | Mampu menganalisis dan mendemonstrasikan menggunakan alat bantu forensik berbasis *Host* Bagian 2 (CPMK 1.6) | 1. *Working with appropriate copies of evidence* 2. *Acquiring a forensically sound image of a computer disk*   *forensic analysis* | Kuliah dan Diskusi *(Role-Play & Simulation, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisis dan mendemonstrasikan menggunakan alat bantu forensik berbasis *Host* Bagian 2 | **Kriteria :** Ketepatan menganalisis dan mendemonstrasikan menggunakan alat bantu forensik berbasis *Host* Bagian 2  **Bentuk :**  Tugas dan Diskusi 1 | 5% |
| 8 | Ujian Tengah Semester (UTS) | | | | | | 25% |  | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] |
| 9 | Mampu menganalisis dan mengevaluasi bukti forensik yang relevan dengan ketentuan hukum dan aturan yang berlaku Bagian 1 (CPMK 1.7) | 1. *Looking for contraband material (such as illicit images or credit card numbers)* 2. *Identifying evidence of malicious code* | Kuliah, Tugas dan Diskusi *(Discovery Learning, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisis dan mengevaluasi bukti forensik yang relevan dengan ketentuan hukum dan aturan yang berlaku Bagian 1 | **Kriteria :** Ketepatan dalam menganalisis dan mengevaluasi bukti forensik yang relevan dengan ketentuan hukum dan aturan yang berlaku Bagian 1  **Bentuk :**  Tugas dan Diskusi 2 | 5% |
| 10 | Mampu menganalisis dan mengevaluasi bukti forensik yang relevan dengan ketentuan hukum dan aturan yang berlaku Bagian 2 (CPMK 1.8) | 1. *Building proof of identity theft* 2. *Building proof of access to confidential information* | Kuliah, Tugas dan Diskusi *(Discovery Learning, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisis dan mengevaluasi bukti forensik yang relevan dengan ketentuan hukum dan aturan yang berlaku Bagian 2 | **Kriteria :** Ketepatan dalam menganalisis dan mengevaluasi bukti forensik yang relevan dengan ketentuan hukum dan aturan yang berlaku Bagian 2  **Bentuk :**  Tugas dan Diskusi 3 | 5% |
| 11 | Mampu  menganalisis, dan mendemonstrasikan teknik forensik dalam pembacaan *log* pada komputer dan jaringan Bagian 1 (CPMK 1.9) | 1. *Capturing network traffic* 2. *How to maintain the value and integrity of evidence* | Kuliah dan Diskusi *(Role-Play & Simulation, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisis, dan mendemonstrasikan teknik forensik dalam pembacaan *log* pada komputer dan jaringan Bagian 1 | **Kriteria :** Ketepatan dalam menganalisis, dan mendemonstrasikan teknik forensik dalam pembacaan *log* pada komputer dan jaringan Bagian 1  **Bentuk:** Tugas dan Diskusi 4 | 5% |
| 12 | Kuis 2 | | | | | | 10% |  | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] |
| 13 | Mampu  menganalisis, dan mendemonstrasikan teknik forensik dalam pembacaan *log* pada komputer dan jaringan Bagian 2 (CPMK 1.10) | 1. *Collection and analysis of network evidence associated with a network event, includes netflow* 2. *Identification of the behavioral characteristics of traffic* | Kuliah dan Diskusi *(Role-Play & Simulation, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1], [2] dan [3] | Ketepatan dalam menganalisis, dan mendemonstrasikan teknik forensik dalam pembacaan *log* pada komputer dan jaringan Bagian 2 | Ketepatan dalam menganalisis, dan mendemonstrasikan teknik forensik dalam pembacaan *log* pada komputer dan jaringan Bagian 2  **Bentuk :**  Diskusi |  |
| 14 | Mampu  menganalisis, dan mendemonstrasikan teknik forensik dalam pembacaan *log* pada komputer dan jaringan Bagian 3 (CPMK 1.11) | 1. *Deep packet inspection* 2. *Analysis of static and dynamic malware* 3. *Email Tracking* 4. *IP Tracking* | Kuliah dan Diskusi *(Discovery Learning, Project Based Learning, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1], [2] dan [3] | Ketepatan dalam menganalisis, dan mendemonstrasikan teknik forensik dalam pembacaan *log* pada komputer dan jaringan Bagian 3 | **Kriteria :** Ketepatan dalam menganalisis, dan mendemonstrasikan teknik forensik dalam pembacaan *log* pada komputer dan jaringan Bagian 3  **Bentuk :**  Diskusi |  |
| 15 | Mampu  menganalisis, dan mendemonstrasikan teknik forensik dalam pembacaan *log* pada komputer dan jaringan Bagian 4 (CPMK 1.12) | 1. *What data was being exfiltrated?* 2. *What services were being exploited?* 3. *Were exploits successful?* 4. *Collection and aggregation of traffic on large networks* | Kuliah dan Diskusi *(Discovery Learning, Project Based Learning, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1], [2] dan [3] | Ketepatan dalam menganalisis, dan mendemonstrasikan teknik forensik dalam pembacaan *log* pada komputer dan jaringan Bagian 4 | **Kriteria :** Ketepatan dalam menganalisis, dan mendemonstrasikan teknik forensik dalam pembacaan *log* pada komputer dan jaringan Bagian 4  **Bentuk :**  Tugas dan Diskusi | 5% |
| 16 | Ujian Akhir Semester (UAS) | | | | | | 35% |

1. Pengalaman Belajar Mahasiswa *(Student Learning Experiences)*

Studi kasus.

1. Bentuk dan Bobot Penilaian
2. Bentuk Penilaian

Tugas = 20%

Kuis = 20%

UTS/MID = 25%

UAS = 35%

1. Bobot penilaian

≥ 85 = A

≥ 70 s.d < 85 = B

≥ 60 s.d < 70 = C

≥ 50 s.d < 60 = D

< 50 = E

1. Buku Sumber *(References)*
2. C. Altheide& H. Carvey. *“Digital Forensics with Open-Source Tools”*, Syngress, 2011. ISBN: 9781597495868
3. Joshi, R., Pilli, E. S. (2016). *“Fundamentals of Network Forensics: A Research Perspective”*. United Kingdom: Springer London.
4. Marsehan, A., Mirza, A. H., & Antoni, D. (2020). *Penilaian Resiko Kejahatan Illegal Content Menggunakan Framework Nist 800-30*. Jurnal Komputer dan Informatika, 22(2), 215-224.