SILABUS

Mata Kuliah : **Forensik Komputer dan Keamanan Siber**
Kode/bobot/Semester : **ISH433 / 3 sks / MK Peminatan Pilihan**

Capaian Pembelajaran Matakuliah (CP-MK):

Setelah mengikuti matakuliah ini mahasiswa:

1. Mampu berkomunikasi antar personal baik dalam bentuk diskusi dan presentasi yang efektif (KH.3);
2. Mampu berpikir analitis, kritis, dan kreatif dalam menyelesaikan permasalahan di bidang Sistem Informasi (KH.1);
3. Mampu melakukan proses evaluasi diri terhadap kelompok kerja yang berada dibawah tanggung jawabnya, dan mampu mengelola pembelajaran secara mandiri; (KU.8);
4. Mampu bertanggungjawab atas pencapaian hasil kerja kelompok dan melakukan supervisi dan evaluasi terhadap penyelesaian pekerjaan yang ditugaskan kepada individu yang berada di bawah tanggungjawabnya; (KU.7)
5. Menyusun deskripsi saintifik hasil kajian dalam bentuk laporan tugas akhir, dan mengunggahnya dalam laman perguruan tinggi;(KU.4)
6. Mampu menunjukkan kinerja mandiri, bermutu, dan terukur; (KU.2)
7. Mampu menerapkan pemikiran logis, kritis, sistematis, dan inovatif dalam konteks pengembangan atau implementasi IPTEK yang memperhatikan dan menerapkan nilai humaniora yang sesuai dengan bidang keahlian Sistem Informasi; (KU.1)
8. Menguasai konsep dasar forensik komputer dan keamanan siber untuk mendukung strategi pemanfaatan sistem informasi dan untuk memenuhi kebutuhan bisnis organisasi. (P.6)
9. Mempunyai keahlian dalam melakukan evaluasi terhadap kepatuhan perusahaan terhadap standar pemanfaatan ICT dan memberikan rekomendasi terhadap pemanfaatan sumber daya IT sesuai dengan kebutuhan bisnis untuk bersaing secara global.(K.4)

Kemampuan yang direncanakan tiap tahapan belajar (Sub-CP-MK):

Setelah mengikuti mata kuliah ini mahasiswa:

1. mampu menjelaskan pengertian, latar belakang, fungsi forensik komputer dan keamanan siber;
2. mampu menjelaskan konsep investigasi untuk mendapatkan digital evidence;
3. mampu menjelaskan konsep, prosedur, strategi dan tools untuk mengakuisisi data forensik;
4. mampu menjelaskan dan mengimplementasikan sistem software forensik
5. mampu menjelaskan dan menggunakan strategi dan tools pada berbagai platform kasus desktop/server, network platform, mobile platform dan aplikasi
6. mampu menjelaskan konsep dan menghasilkan dokumentasi pada aktivitas forensik yang mencakup aspek hukum legal dan saksi ahli
7. mampu menjelaskan konsep dan berbagai aspek dasar keamanan siber
8. mampu menjelaskan aristektur keamanan siber
9. mampu menjelaskan implementasi dan operasi keamanan siber
10. mampu menjelaskan pertahanan siber yang mencakup membangun pertahanan siber dan respon insiden
11. mampu menjelaskan pengelolaan pertahanan siber yang mencakup manajemen krisis dan asesmen pertahanan siber
12. mampu menjelaskan dan menyusun program keamanan siber enterprise

Pokok Bahasan (*Subject Matter*):

Pengertian dan fungsi forensik komputer, pengertian dan fungsi keamanan siber, konsep investigasi pada digital evidence, akuisisi data forensik yang mencakup konsep, prosedur, strategi dan tools, pengimplementasian sistem software forensik, implementasi strategi dan tools pada contoh kasus berbagai platform, aspek dokumentasi legal dan saksi ahli, pengertian dan fungsi aspek dasar keamanan siber, pengertian dan fungsi implementasi dan operasi keamanan siber, konsep pertahanan siber dan respon insiden, konsep manajemen krisis dan asesmen pertahanan siber, penyusunan keamanan siber enterprise.

Pustaka Utama:

1. Brook, Charles L,"CHFI : Computer Hacking Forensic Investigator Certification" McGrawHill Osborne Media, 2014
2. Donaldson, Scott,"EnterpriseCybersecurity How to Build a SuccesfulCyberdefense Program", Apress, 2013

Pustaka Penunjang :

1. al-Azhar, M Nuh,"Digital Forensic: Panduan Praktis Investigasi Komputer", Penerbit Salemba Infotek, 2012

KomponenNilaiAkhir:

UAS 25%, Praktikum Mandiri 25%, Tugas 25%, UTS 25%