

YAYASAN SIMRS KHANZA INDONESIA

CYBER SCHOOL

BUILD SKILLS

NETWORK & PROGRAMMING

WWW.YASKI.OR.ID

START JANUARI 2023

A. PENDAHULUAN

Kursus keamanan siber saat ini dibutuhkan oleh talenta digital yang berkarir di bidang Teknologi Informasi. Salah satu alasan pentingnya profesi ini adalah meluasnya pelanggaran data, sehingga Rumah Sakit membutuhkan seseorang yang dapat melindungi sistem komputer, aset perusahaan, dan aset pengguna dari berbagai serangan kejahatan dunia maya. Menariknya, prospek karir di bidang ini sangat dibutuhkan, dan tantangan yang didapatkan tidak sespektakuler profesi IT lainnya.

Faktanya, kebutuhan akan profesional untuk mengatasi kejahatan dunia maya berkembang pesat, bahkan kebutuhan terhadap keamanan dunia maya di seluruh dunia meningkat hingga 350% dalam setahun terakhir. Selain itu, peneliti keamanan siber memperkirakan bahwa jumlah persyaratan profesional di bidang ini akan meningkat selama lima tahun ke depan. Ada beberapa posisi keamanan siber yang sering dicari perusahaan, antara lain analis keamanan siber, insinyur keamanan, analis keamanan, penguji penetrasi, peretas legal bersertifikasi, kepala petugas keamanan, dan lainnya.

Akan tetapi, untuk memulai karir di bidang keamanan siber, setidaknya harus memiliki keterampilan, pengetahuan, dan portofolio pendukung. Semua prasyarat yang dapat menunjang peserta profesional di bidang ini dapat diperoleh peserta yang telah menyelesaikan kursus keamanan siber. Meskipun pesertanya adalah orang-orang yang tidak dapat belajar sendiri dan awam perihal IT, dengan mengikuti kursus ini akan sangat membantu peserta dalam perjalanan menuju karir di bidang keamanan siber. Salah satu kursus keamanan siber untuk Sistem Rumah Sakit yang paling direkomendasikan di Indonesia adalah **Yaski School of CyberSec**.

Berdasarkan Peraturan Menteri Kesehatan Republik Indonesia Nomor 18 Tahun 2022 Tentang Penyelenggaraan Satu Data Bidang Kesehatan Melalui Sistem Informasi Kesehatan yang berisi Walidata Kesehatan, Walidata, Pengguna Data, Standar Data Kesehatan, Metadata, Interoperabilitas Data, Kode Referensi, Data Kesehatan Prioritas, Kriteria Data Kesehatan, Informasi Kesehatan dan berbagai hal penting lainnya yang sangat penting dijaga kerahasiaan, ketersediaan dan kehandalan dari data atau informasi yang diproses oleh Sistem tersebut. Oleh karena itu, sudah seharusnya Pihak

Rumah Sakit lebih prioritaskan untuk meningkatkan keahlian dan keterampilan dari Sumber Daya Manusia di Bidang Teknologi Informasi yang dimiliki oleh masing-masing Rumah Sakit.

Yaski School of CyberSec:

Yaski School of CyberSec adalah bootcamp yang menawarkan kursus online tentang berbagai keterampilan digital, seperti: Kursus Keamanan Data, Pemasaran Digital, Data Science, Fullstack Developer, Desain UI/UX, Copywriting, dan Keterampilan Digital lainnya. Semua orang tanpa memandang latar belakang dapat berpartisipasi dalam kursus Yaski School of CyberSec. Mulai dari pelajar, pengusaha, hingga profesional di berbagai bidang.

Yaski School of CyberSec tidak hanya menawarkan kursus untuk umum, tetapi juga pelatihan untuk Rumah Sakit dan Layanan Kesehatan di Indonesia. Menariknya, **Yaski School of CyberSec** akan membantu dan membimbing para peserta agar mereka dapat memperoleh keterampilan digital, dengan berbagai fasilitas, kurikulum, portofolio yang dipimpin oleh Instruktur berpengalaman dan bersertifikasi Internasional yang siap membantu peserta untuk berkarir di bidang digital, bahkan tanpa latar belakang linier.

Mini Bootcamp Cyber Security:

Prospek karir cybersecurity sangat dibutuhkan, bahkan beberapa perusahaan termasuk BUMN, Lembaga Pemerintah, Rumah Sakit, Organisasi Nirlaba, Perusahaan swasta dan Organisasi Kecil hingga Besar sedang memerlukan profesional cybersecurity. Oleh karena itu, **Yaski School of CyberSec** menawarkan kursus yang dapat diambil oleh siapa saja tanpa latar belakang khusus.

CyberSecurity Mini Bootcamp memandu peserta untuk memahami pengetahuan dan praktik pengujian penetrasi keamanan siber dan untuk memahami langkah-langkah dan praktik terbaik untuk menjadi pemburu bug pemula yang baik dan profesional. Melalui kursus ini, peserta dapat melakukan uji penetrasi, mendokumentasikan kerentanan dalam laporan bug bounty, dan membagikan hasil bug dengan pemilik sistem ataupun pengguna sistem.

Akhir dari Mini Bootcamp adalah peserta memiliki keahlian menjaga keamanan data dan informasi dari mulai perencanaan Data Kesehatan, pengumpulan Data Kesehatan, pemeriksaan Data Kesehatan, pengolahan Data Kesehatan, penyimpanan Data Kesehatan, pengamanan Data Kesehatan, penyebarluasan Data Kesehatan, dan penggunaan Data Kesehatan sehingga diharapkan pihak Rumah Sakit mempunyai Sumber Daya Manusia Profesional dan bersertifikasi Internasional di Bidang IT yang mampu menjaga kerahasiaan, kehandalan dan ketersediaan data.

B. FASILITAS

Jika peserta mengikuti Mini Bootcamp Cyber Security **Yaski School of CyberSec**, peserta akan mendapatkan berbagai fasilitas pendukung yang dapat membantu mempermudah peserta dalam proses pembelajaran, diantaranya :

1. Sertifikat Yaski School of CyberSec*
2. Learning performance report
3. Bug bounty report portfolio
4. 3 mini projects
5. International certification**
6. Cybersecurity analyst sharing session
7. Career coaching and mentoring
8. Professional branding
9. Interactive review by tutor
10. Industry-based curriculum
11. Focus on practice
12. Lifetime access to learning ecosystem.

* Certified Healthcare Information Security Analyst (CHISA)

**Jika lulus Ujian Internasional.

SISTEM PEMBELAJARAN

1. Luring ZOOM
2. Web E-Learning
3. Exam
4. Graduation

5. Modul
6. Project
7. Grup Telegram

FOCUS STUDY

1. Network Skills
2. Linux Skills
3. Computer Skills
4. Programming Skills
5. SQL Skills
6. Hardware Knowledge
7. Knowledge in Reverse Engineering
8. Cryptography

C. WAKTU

GELOMBANG 1 Start Januari 2022

1. Sesi 1 Januari : 16x Pertemuan
3x Pertemuan Materi dan 1x Pertemuan Diskusi
2. Sesi 2 Februari : 16x Pertemuan
3x Pertemuan Materi dan 1x Pertemuan Diskusi
3. Sesi 3 Maret : 16x Pertemuan
3x Pertemuan Materi dan 1x Pertemuan Diskusi
4. Sesi 4 April : 16x Pertemuan
3x Pertemuan Materi dan 1x Pertemuan Diskusi
5. Sesi 5 Mei : 16x Pertemuan
3x Pertemuan Materi dan 1x Pertemuan Diskusi
6. Sesi 6 Juni : 16x Pertemuan
3x Pertemuan Materi dan 1x Pertemuan Diskusi

GELOMBANG 2 Start Februari 2022

1. Sesi 1 Februari : 16x Pertemuan
3x Pertemuan Materi dan 1x Pertemuan Diskusi
2. Sesi 2 Maret : 16x Pertemuan

- | | |
|-----------------|--|
| | 3x Pertemuan Materi dan 1x Pertemuan Diskusi |
| 3. Sesi 3 April | : 16x Pertemuan |
| | 3x Pertemuan Materi dan 1x Pertemuan Diskusi |
| 4. Sesi 4 Mei | : 16x Pertemuan |
| | 3x Pertemuan Materi dan 1x Pertemuan Diskusi |
| 5. Sesi 5 Juni | : 16x Pertemuan |
| | 3x Pertemuan Materi dan 1x Pertemuan Diskusi |
| 6. Sesi 6 Juli | : 16x Pertemuan |
| | 3x Pertemuan Materi dan 1x Pertemuan Diskusi |

JAM DARING DIMULAI PUKUL 19.00 – 22.00 WIB Setiap Pertemuan

D. BIAYA

- | | |
|---------------------|--|
| 1. COST BOOKING | : Rp. 500.000,- |
| | : Sisanya Akan ditagihkan di Tgl 5 |
| 2. COST SESSION | : Rp. 1.500,000,- /sesi x 6 Bulan |
| | : Pembayaran Maksimal Tgl 10 |
| | Pembayaran akan ditagihan setiap bulan |
| | Dikirimkan secara E-Mail |
| 3. COST GRADUATION | : Mengikuti Tempat Kegiatan |
| 4. COST CERTIFICATE | : Mengikuti Kurs \$ Setelah Lulus Sesi |

**To : Bank BNI Cab. Kediri Nomor 0714514494 a/n Yayasan SIMRS
Khanza Indonesia**

E. REGISTRASI

1. Link Pendaftaran Maksimal Tgl 25 Desember 2022 :
<https://bit.ly/CyberSecuritySchoolYASKI>
2. Pretest hasil akan menentukan kelas Basic sama Non Basic pada email setelah melakukan booking pendaftaran.

YAYASAN SIMRS KHANZA INDONESIA

Sekretariat :

Perumahan Bunga Lestari Blok D. 15 RT/RW. 016/005

Desa Kedungarum Kec./Kab. Kuningan, Provinsi Jawa Barat, Indonesia

HP : 082138143546

Website : www.yaski.or.id Email : aski.khanzaindonesia@gmail.com



DOSEN DAN PRAKTISI




**Dr. SEPTIAN RHENO W, M. Sc, M. Kom, M. Eng, Ph. D, CEH, ECSA,
CNSS, CSFPC, LCSPC, CCT, ACA CLOUD SECURITY**



YAYASAN SIMRS KHANZA
SCHOOL OF CYBERSEC

Perumahan Bunga Lestari Blok D. 15 RT/RW. 016/005. Desa Kedungarum Kec./Kab. Kuningan, Provinsi Jawa Barat, Indonesia.
 Tel: +62-821 381 435 46

RENCANA PEMBELAJARAN SEMESTER (RPS)

Nama Mata Kuliah	Kode Mata Kuliah	Bobot (sks)	Semester	Tgl Penyusunan
Dasar - Dasar Keamanan Komputer	CBS201	3	2	20 November 2022
Otorisasi	Nama Koordinator Pengembang RPS	Koordinator Bidang Keahlian (Jika Ada)	INSTRUKTUR	
	 Septian Rheno Widiyanto, S.Kom., M.Eng., M.Kom, CEH, ECSA	 Septian Rheno Widiyanto, S.Kom., M.Eng., M.Kom, CEH, ECSA	 Septian Rheno Widiyanto, S.Kom., M.Eng., M.Kom, CEH, ECSA	

Capaian Pembelajaran (CP)	CPL-SCHOOL OF CYBERSEC (Capaian Pembelajaran Lulusan) Yang Dibebankan Pada Mata Kuliah	
	1	Menjelaskan dan menerapkan dasar-dasar keamanan komputer.
	2	Menjelaskan dan menerapkan keamanan komputer dan jaringan.
	3	Menjelaskan cara membangun perangkat lunak yang aman.
	CPMK (Capaian Pembelajaran Mata Kuliah)	
	CPMK1	Siswa/i mampu memahami bagaimana penerapan keamanan informasi.
	CPMK2	Siswa/i mampu memahami bagaimana penerapan keamanan dengan menggunakan antivirus.
	CPMK3	Siswa/i mampu memahami bagaimana penerapan enkripsi data.
	CPMK4	Siswa/i mampu memahami bagaimana penerapan backup terhadap data dan penerapan disaster recovery.
	CPMK5	Siswa/i mampu memahami bagaimana penerapan backup terhadap data dan penerapan disaster recovery.
	CPMK6	Siswa/i mampu memahami bagaimana penerapan keamanan penggunaan media internet.
	CPMK7	Siswa/i mampu memahami bagaimana penerapan keamanan koneksi jaringan komputer.
	CPMK8	Siswa/i mampu memahami bagaimana penerapan keamanan Transaksi Online.
	CPMK9	Siswa/i mampu memahami bagaimana penerapan keamanan Komunikasi Email.
	CPMK10	Siswa/i mampu memahami bagaimana penerapan Social Engineering dan Pencurian Identitas.
	CPMK11	Siswa/i mampu memahami bagaimana penerapan Keamanan di Social Media.
	CPMK12	Siswa/i mampu memahami bagaimana penerapan Keamanan Informasi dan Kepatuhan Hukum.
	CPMK13	Siswa/i mampu memahami bagaimana penerapan Keamanan Perangkat Mobile.

Diskripsi Singkat MK	Mata Kuliah ini mengajarkan tentang fundamental Keamanan informasi, antivirus, enkripsi data, backup data dan disaster recovery, keamanan internet, keamanan koneksi jaringan, keamanan komunikasi email, social engineering dan pencurian identitas, keamanan sosial media, keamanan informasi dan kepatuhan hukum, dan keamanan perangkat mobile.	
Bahan Kajian / Materi Pembelajaran	<ol style="list-style-type: none"> 1. Fundamental Keamanan Informasi; Fundamental Keamanan Informasi, Melindung Komputer dengan Antivirus. 2. Antivirus; Melindung Komputer dengan Antivirus. 3. Enkripsi Data. 4. Backup Data dan Disaster Recovery. 5. Keamanan Internet. 6. Keamanan Koneksi Jaringan. 7. Keamanan Transaksi Online. 8. Keamanan Komunikasi Email. 9. Social Engineering dan Pencurian Identitas. 10. Keamanan di Social Media. 11. Keamanan Informasi dan Kepatuhan Hukum. 12. Keamanan Perangkat Mobile. 	
Daftar Referensi	Utama:	
	(1) Certified Secure Computer User (CSCU) Module by. EC – Council.	
	Pendukung:	

Nama Instruktur	Septian Rheno Widiyanto, S.Kom., M.Eng., M.Kom, CEH, ECSA.
Mata kuliah prasyarat (Jika ada)	Sistem Operasi.

Minggu Ke-	Sub-CPMK (Kemampuan akhir yg direncanakan)	Bahan Kajian (Materi Pembelajaran)	Bentuk dan Metode Pembelajaran [Media & Sumber Belajar]	Estimasi Waktu (Menit)	Pengalaman Belajar Siswa/i YASKI School of CyberSec	Penilaian		
						Kriteria & Bentuk	Indikator	Bobot (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
1	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan keamanan informasi.	1. Kontrak Pembelajaran 2. Fundamental Keamanan Informasi.	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec memahami penerapan keamanan informasi.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam menyebutkan penerapan keamanan informasi.	5
2	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan keamanan sistem operasi.	1. Mengamankan Sistem Operasi.	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec dapat menerapkan pengamanan sistem operasi.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam mengamankan sistem operasi.	5

3	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan keamanan dengan menggunakan antivirus.	1. Antivirus.	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengetahui penggunaan antivirus sebagai pengamanan komputer.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam mengenali jenis-jenis dan cara kerja antivirus.	5
4	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan enkripsi data.	1. Enkripsi Data.	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengetahui dan mempraktekkan penerapan enkripsi data.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam penerapan enkripsi data.	5
5	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan backup terhadap data dan penerapan disaster recovery.	1. Backup Data dan Disaster Recovery.	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengimplementasikan penerapan backup terhadap data dan penerapan disaster recovery.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam mengenali penerapan backup terhadap data dan penerapan disaster recovery.	5

6	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan backup terhadap data dan penerapan disaster recovery.	1. Backup Data dan Disaster Recovery.	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengimplementasikan penerapan backup terhadap data dan penerapan disaster recovery.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam mengenali penerapan backup terhadap data dan penerapan disaster recovery.	5
7	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan keamanan penggunaan media internet.	1. Keamanan Internet	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengimplementasikan penerapan keamanan penggunaan media internet	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam implementasi penerapan keamanan penggunaan media internet	5
8	Ujian Tengah Semester							15
9	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan keamanan koneksi	1. Keamanan Koneksi Jaringan.	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengimplementasikan penerapan keamanan koneksi jaringan komputer.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam implementasi penerapan keamanan koneksi jaringan komputer.	5

	jaringan komputer.							
10	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan keamanan transaksi online.	1. Keamanan Transaksi Online.	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengimplementasikan penerapan keamanan transaksi online.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam implelementasi penerapan keamanan transaksi online.	5
11	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan keamanan komunikasi email.	1. Keamanan Komunikasi Email.	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengimplementasikan penerapan keamanan komunikasi email.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam implementasi penerapan keamanan komunikasi email.	5

12	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan social engineering dan pencurian identitas.	1. Social Engineering dan Pencurian Identitas.	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec membuat program dengan mengimplementasikan penerapan social engineering dan pencurian identitas.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam implementasi penerapan social engineering dan pencurian identitas.	5
13	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan keamanan di social media.	1. Keamanan di Social Media.	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengimplementasikan penerapan keamanan di social media.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam implementasi penerapan keamanan di social media.	5
14	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan keamanan informasi dan kepatuhan hukum.	1. Keamanan informasi dan kepatuhan hukum.	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengimplemntasikan penerapan keamanan informasi dan kepatuhan hukum.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam implementasi penerapan keamanan informasi dan kepatuhan hukum.	5

15	Siswa/i YASKI School of CyberSec mampu lulus Exam CSCU (Certified Secure Computer User)	1. Preparation Exam CSCU	<ul style="list-style-type: none"> - Online Exam - Minimum Poin: 70%. - Test Format: Pilihan Ganda. - Jumlah Pertanyaan: 50. 	120	Siswa/i YASKI School of CyberSec melakukan Exam CSCU secara online.	Exam	Ketepatan dan kesesuaian dalam mengisi soal exam CSCU.	20
16	Ujian Akhir Semester							

Catatan:

1. Capaian Pembelajaran Lulusan (CPL) adalah kemampuan yang dimiliki oleh setiap lulusan **YASKI School of CyberSec** yang merupakan internalisasi dari sikap, penguasaan pengetahuan dan ketrampilan sesuai dengan jenjang prodinya yang diperoleh melalui proses pembelajaran.
2. CPL yang dibebankan pada mata kuliah adalah beberapa capaian pembelajaran lulusan program studi (CPL) yang digunakan untuk pembentukan/ pengembangan sebuah mata kuliah yang terdiri dari aspek sikap, ketrampilan umum, ketrampilan khusus dan pengetahuan.
3. CP Mata kuliah (CPMK) adalah kemampuan yang dijabarkan secara spesifik dari CPL yang dibebankan pada mata kuliah, dan bersifat spesifik terhadap bahan kajian atau materi pembelajaran mata kuliah tersebut.
4. Sub-CP Mata kuliah (Sub-CPMK) adalah kemampuan yang dijabarkan secara spesifik dari CPMK yang dapat diukur atau diamati dan merupakan kemampuan akhir yang direncanakan pada tiap tahap pembelajaran, dan bersifat spesifik terhadap materi pembelajaran mata kuliah tersebut.
5. Kriteria Penilaian adalah patokan yang digunakan sebagai ukuran atau tolok ukur ketercapaian pembelajaran dalam penilaian berdasarkan indikator-indikator yang telah ditetapkan. Kriteria penilaian merupakan pedoman bagi penilai agar penilaian konsisten dan tidak bias. Kriteria dapat berupa kuantitatif ataupun kualitatif.
6. Indikator penilaian kemampuan dalam proses maupun hasil belajar Siswa/i **School of CyberSec** adalah pernyataan spesifik dan terukur yang mengidentifikasi kemampuan atau kinerja hasil belajar Siswa/i **YASKI School of CyberSec** yang disertai bukti-bukti.






YAYASAN SIMRS KHANZA

SCHOOL OF CYBERSEC

Perumahan Bunga Lestari Blok D. 15 RT/RW. 016/005. Desa Kedungarum Kec./Kab. Kuningan, Provinsi Jawa Barat, Indonesia.
Tel: +62-821 381 435 46

RENCANA PEMBELAJARAN SEMESTER (RPS)

Nama Mata Kuliah	Kode Mata Kuliah	Bobot (sks)	Semester	Tgl Penyusunan
Forensika Digital	CBS202	3	2	20 November 2022
Otorisasi	Nama Koordinator Pengembang RPS	Koordinator Bidang Keahlian (Jika Ada)	INSTRUKTUR	
	 Septian Rheno Widiyanto, S.Kom., M.Eng., M.Kom, CEH, ECSA	 Septian Rheno Widiyanto, S.Kom., M.Eng., M.Kom, CEH, ECSA	 Septian Rheno Widiyanto, S.Kom., M.Eng., M.Kom, CEH, ECSA	

Capaian Pembelajaran (CP)	CPL-SCHOOL OF CYBERSEC (Capaian Pembelajaran Lulusan) Yang Dibebankan Pada Mata Kuliah	
	1	Menjelaskan dan menerapkan dasar-dasar ilmu forensik.
	2	Menjelaskan dan menerapkan dasar digital forensik, windows forensik, forensik jaringan, dan forensik perangkat mobile.
	3	Menjelaskan cara membuat Laporan investigasi.
	CPMK (Capaian Pembelajaran Mata Kuliah)	
	CPMK1	Siswa/i mampu memahami bagaimana penerapan ilmu forensik.
	CPMK2	Siswa/i mampu memahami bagaimana penerapan digital forensik, windows forensik, forensik jaringan, dan forensik perangkat mobile.
	CPMK3	Siswa/i mampu memahami bagaimana penerapan digital evidence.
	CPMK4	Siswa/i mampu memahami bagaimana penerapan first responder procedures.
	CPMK5	Siswa/i mampu memahami bagaimana penerapan forensik sistem operasi windows.
	CPMK6	Siswa/i mampu memahami bagaimana penerapan akusisi data dan duplikasi.
	CPMK7	Siswa/i mampu memahami bagaimana penerapan perbaikan file dan partisi yang terhapus.
	CPMK8	Siswa/i mampu memahami bagaimana penerapan investigasi forensik menggunakan AccessData FTK dan EnCase.
	CPMK9	Siswa/i mampu memahami bagaimana penerapan steganografi dan forensik file gambar.
	CPMK10	Siswa/i mampu memahami bagaimana penerapan aplikasi crack password & log.
	CPMK11	Siswa/i mampu memahami bagaimana penerapan forensik jaringan, investigasi trafik jaringan & log.
	CPMK12	Siswa/i mampu memahami bagaimana penerapan investigasi jaringan wireless dan serangan web.
	CPMK13	Siswa/i mampu memahami bagaimana penerapan track email & investigasi kejahatan email.
	CPMK14	Siswa/i mampu memahami bagaimana penerapan forensik perangkat mobile.
	CPMK15	Siswa/i mampu memahami bagaimana penerapan laporan forensika digital.

Diskripsi Singkat MK	<p>Mata Kuliah ini mengajarkan tentang dasar-dasar ilmu forensik, dasar digital forensik, windows forensik, forensik jaringan, dan forensik perangkat mobile, digital evidence, first responder procedures, forensik sistem operasi windows, akusisi data & duplikasi, perbaikan file dan partisi yang terhapus, investigasi forensik menggunakan AccessData FTK dan EnCase, steganografi dan forensik file gambar, aplikasi crack password & log, forensik jaringan, investigasi trafik jaringan & log, investigasi jaringan wireless dan serangan web, track email & investigasi kejahatan email, track email & investigasi kejahatan email, forensik perangkat mobile, laporan forensika digital.</p>
Bahan Kajian / Materi Pembelajaran	<ol style="list-style-type: none"> 1. Dasar-dasar ilmu forensik. 2. Dasar digital forensik, windows forensik, forensik jaringan, dan forensik perangkat mobile. 3. Digital evidence. 4. First responder procedures. 5. Forensik sistem operasi windows. 6. Akusisi data dan duplikasi. 7. Perbaikan file dan partisi yang terhapus. 8. Investigasi forensik menggunakan AccessData FTK dan EnCase. 9. Steganografi dan forensik file gambar. 10. Aplikasi crack password & log. 11. Forensik jaringan, investigasi trafik jaringan & log. 12. Investigasi jaringan wireless dan serangan web. 13. Track email & investigasi kejahatan email. 14. Forensik perangkat mobile. 15. Laporan forensika digital.

Daftar Referensi	Utama:	
	(1) Certified Hacking Forensic Investigator (CHFI) Module by. EC – Council.	
	Pendukung:	
Nama Instruktur	Septian Rheno Widiyanto, S.Kom., M.Eng., M.Kom, CEH, ECSA.	
Mata kuliah prasyarat (Jika ada)	Sistem Operasi.	

Minggu Ke-	Sub-CPMK (Kemampuan akhir yg direncanakan)	Bahan Kajian (Materi Pembelajaran)	Bentuk dan Metode Pembelajaran [Media & Sumber Belajar]	Estimasi Waktu (Menit)	Pengalaman Belajar Siswa/i YASKI School of CyberSec	Penilaian		
						Kriteria & Bentuk	Indikator	Bobot (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
1	Siswa/i YASKI School of CyberSec mampu memahami bagaimana dasar-dasar ilmu forensik.	1. Kontrak Pembelajaran 2. Dasar-dasar ilmu forensik	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec memahami penerapan ilmu forensik..	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam menyebutkan penerapan ilmu forensik..	5

2	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan dasar-dasar digital forensik, windows forensik, forensik jaringan, dan forensik perangkat mobile.	<ol style="list-style-type: none"> 1. Dasar-dasar digital forensik 2. Windows forensik 3. Forensik jaringan 4. Forensik perangkat mobile 	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec dapat menerapkan pengamanan digital forensik, windows forensik, forensik jaringan, dan forensik perangkat mobile.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam mengamankan digital forensik, windows forensik, forensik jaringan, dan forensik perangkat mobile.	5
3	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan digital evidence.	<ol style="list-style-type: none"> 1. Digital Evidence 	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengetahui dan mempraktekkan penerapan digital evidence.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam mengenali jenis-jenis dan cara digital evidence.	5
4	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan first responder procedures.	<ol style="list-style-type: none"> 1. First responder procedures 	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengetahui dan mempraktekkan penerapan first responder procedures.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam penerapan first responder procedures.	5

5	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan forensik sistem operasi windows.	1. Forensik sistem operasi windows	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengimplementasikan penerapan forensik sistem operasi windows.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam mengenali penerapan backup terhadap data dan penerapan forensik sistem operasi windows..	5
6	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan akusisi data dan duplikasi.	1. Akusisi data dan duplikasi	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengimplementasikan penerapan akusisi data dan duplikasi.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam mengenali penerapan backup terhadap data dan penerapan akusisi data dan duplikasi.	5
7	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan perbaikan file dan partisi yang terhapus.	1. Perbaikan file dan partisi yang terhapus	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengimplementasikan penerapan perbaikan file dan partisi yang terhapus.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam implementasi penerapan perbaikan file dan partisi yang terhapus.	5
8	Ujian Tengah Semester							15

9	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan investigasi forensik menggunakan AccessData FTK dan EnCase.	1. Investigasi forensik menggunakan AccessData FTK dan EnCase.	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengimplementasikan penerapan investigasi forensik menggunakan AccessData FTK dan EnCase.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam implementasi penerapan investigasi forensik menggunakan AccessData FTK dan EnCase.	5
10	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan steganografi dan forensik file gambar	1. Steganografi 2. Forensik file gambar.	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengimplementasikan penerapan steganografi dan forensik file gambar.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam implementasi penerapan steganografi dan forensik file gambar.	5
11	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan aplikasi crack password & log.	1. Aplikasi crack password & log.	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengimplementasikan penerapan aplikasi crack password & log.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam implementasi penerapan aplikasi crack password & log.	5

12	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan forensik jaringan, investigasi trafik jaringan & log.	1. Forensik jaringan 2. Investigasi trafik jaringan & log	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec membuat program dengan mengimplementasikan penerapan forensik jaringan, investigasi trafik jaringan & log.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam implementasi penerapan forensik jaringan, investigasi trafik jaringan & log.	5
13	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan investigasi jaringan wireless dan serangan web.	1. Investigasi jaringan wireless 2. Serangan web.	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengimplementasikan penerapan investigasi jaringan wireless dan serangan web	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam implementasi penerapan investigasi jaringan wireless dan serangan web.	5
14	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan track email & investigasi kejahatan email.	1. Track email & investigasi kejahatan email.	Tatap muka, ceramah, diskusi, dan praktikum.	120	Siswa/i YASKI School of CyberSec mengimplemntasikan penerapan track email & investigasi kejahatan email.	Latihan Soal, Umpan Balik Pertanyaan dan Keaktifan diskusi.	Ketepatan dan kesesuaian dalam implementasi penerapan track email & investigasi kejahatan email.	5

15	Siswa/i YASKI School of CyberSec mampu memahami bagaimana penerapan forensik perangkat mobile dan membuat laporan forensika digital.	1. Forensik perangkat mobile. 2. Laporan forensika digital.	- Online Exam - Minimum Poin: 70%. - Test Format: Pilihan Ganda. - Jumlah Pertanyaan: 150.	120	Siswa/i YASKI School of CyberSec mengimplemntasikan penerapan forensik perangkat mobile dan membuat laporan forensika digital.	Exam	Ketepatan dan kesesuaian dalam mengisi soal exam CSCU.	5
16	Siswa/i YASKI School of CyberSec mampu lulus Exam CHFI (Certified Hacking Forensic Investigation)	1. Preparation Exam CHFI (Certified Hacking Forensic Investigation)	- Online Exam - Minimum Poin: 70%. - Test Format: Pilihan Ganda. - Jumlah Pertanyaan: 150.	240	Siswa/i YASKI School of CyberSec melakukan Exam CHFI secara online.	Exam	Ketepatan dan kesesuaian dalam mengisi soal exam CHFI.	10
17	Ujian Akhir Semester							5

Catatan:

1. Capaian Pembelajaran Lulusan (CPL) adalah kemampuan yang dimiliki oleh setiap lulusan **YASKI School of CyberSec** yang merupakan internalisasi dari sikap, penguasaan pengetahuan dan ketrampilan sesuai dengan jenjang prodinya yang diperoleh melalui proses pembelajaran.
2. CPL yang dibebankan pada mata kuliah adalah beberapa capaian pembelajaran lulusan program studi (CPL) yang digunakan untuk pembentukan/pengembangan sebuah mata kuliah yang terdiri dari aspek sikap, ketrampilan umum, ketrampilan khusus dan pengetahuan.
3. CP Mata kuliah (CPMK) adalah kemampuan yang dijabarkan secara spesifik dari CPL yang dibebankan pada mata kuliah, dan bersifat spesifik terhadap bahan kajian atau materi pembelajaran mata kuliah tersebut.
4. Sub-CP Mata kuliah (Sub-CPMK) adalah kemampuan yang dijabarkan secara spesifik dari CPMK yang dapat diukur atau diamati dan merupakan kemampuan akhir yang direncanakan pada tiap tahap pembelajaran, dan bersifat spesifik terhadap materi pembelajaran mata kuliah tersebut.
5. Kriteria Penilaian adalah patokan yang digunakan sebagai ukuran atau tolok ukur ketercapaian pembelajaran dalam penilaian berdasarkan indikator-indikator yang telah ditetapkan. Kriteria penilaian merupakan pedoman bagi penilai agar penilaian konsisten dan tidak bias. Kriteria dapat berupa kuantitatif ataupun kualitatif.
6. Indikator penilaian kemampuan dalam proses maupun hasil belajar Siswa/i **School of CyberSec** adalah pernyataan spesifik dan terukur yang mengidentifikasi kemampuan atau kinerja hasil belajar Siswa/i **YASKI School of CyberSec** yang disertai bukti-bukti.