

COURSE SYLLABUS

INFORMATION TECHNOLOGY AND COMMUNICATIONS FORENSICS

1. Program identification details

1.1 Higher education institution	Universitatea „OVIDIUS”, Constanța
1.2 Faculty	Facultata de Matematică și Informatică
1.3 Department	Matematică și Informatică
1.4 Field of studies	Informatică
1.5 Cycle of studies (degree)	Master
1.6 Degree program/qualification	Securitate Cibernetică și Învățare Automată
1.7 Academic year	2025-2026

2. Course identification details

2.1 Course title	Tehnologia Informației și Criminalistică Digitală						
2.2 Course code	FMI.CSML.II.1.10						
2.3 Instructor	Conf. Univ. Dr. Mihailescu Marius Iulian						
2.4 Teaching assistant	Conf. Univ. Dr. Mihailescu Marius Iulian						
2.5 Year	II	2.6 Semester	1	2.7. Evaluation type	E	2.8 Course type */**	DAP/DO

* DF – fundamental course, DD – field course, DS – specialty course, DC – complementary course, DAP – advanced study course, DSI – synthesis course, DCA – advanced knowledge course.

** DI – mandatory course; DO – optional course.

3. Estimated workload (hours per semester)

3.1 Number of teaching hours/week	2	of which: 3.2 course	1	3.3 applications***	1
3.4 Total of teaching hours within the program/semester	28	of which: 3.5 lecture	14	3.6 seminar	14
3.7 Student workload for individual study					97
Distribution of workload					[hours]
Studiu individual al manualelor, ghidurilor/cartelor de lectură, bibliografiei și notițelor					28
Cercetare suplimentară (bibliotecă, resurse electronice, muncă de teren)					20
Teme (pregătirea prezentărilor de seminar, portofoliilor, eseurilor critice, lucrărilor de cercetare etc.)					28
Consultații individuale (opționale)					14
Evaluări / examene					4
Alte activități					3
3.8 Total hours per semester	28+97=125				
3.9 Number of credits	5				

*** S - seminar; L - laboratory; P - project

4. Prerequisites (where applicable)

4.1 Curriculum-related	-
4.2 Skills-related	Gândire logică și abilități de rezolvare algoritmică a problemelor

5. Necessary requirements for optimum teaching and learning (where applicable)

5.1. For running the course	Sală de clasă disponibilă
5.2. For running the seminar / laboratory /project <i>*The type is to be chosen according to the discipline</i>	Sală de clasă disponibilă / sală de laborator disponibilă

6. Course objectives

6.1 The general objective of the course	Dobândirea cunoștințelor, înțelegerii și utilizării adecvate a conceptelor/metodelor și instrumentelor software/hardware care pot fi utilizate în criminalitatea cibernetică.
6.2 Specific objectives	Dobândirea abilităților necesare în aplicarea tehnicilor de protecție a sistemelor informatice. Dobândirea abilităților necesare pentru crearea de aplicații software robuste și sigure. Dobândirea abilităților în colectarea/analiza datelor și obținerea de dovezi relevante în urma unui incident de criminalitate cibernetică/criminalitate cibernetică. Dobândirea abilităților necesare în utilizarea instrumentelor software specifice securității sistemelor informatice și securității datelor.

7. Learning outcomes

Knowledge	<p>După finalizarea cu succes a acestui curs, studenții vor dobândi cunoștințe teoretice și practice avansate despre principiile, metodologiile și tehnologiile criminalistice digitale aplicate tehnologiei informației și sistemelor de comunicații. Vor înțelege cadrele juridice, etice și procedurale care guvernează colectarea, conservarea, analiza și prezentarea dovezilor digitale, atât la nivel național, cât și internațional.</p> <p>Studenții vor dezvolta cunoștințe aprofundate despre criminalistica informatică și de rețea, inclusiv structurile sistemelor de fișiere, artefactele sistemului de operare și analiza traficului de rețea. Vor înțelege procesele criminalistice implicate în răspunsul la incidente, achiziția de dovezi, gestionarea lanțului de custodie și imagistica criminalistică, asigurând integritatea și admisibilitatea dovezilor digitale.</p> <p>Cursul va oferi o perspectivă cuprinzătoare asupra criminalisticii comunicațiilor, acoperind investigarea canalelor de comunicații digitale, cum ar fi e-mailul, mesageria instantanee, VoIP, dispozitivele mobile și platformele de socializare. Studenții vor învăța protocoalele subiacente, formatele de date și structurile de metadata relevante pentru examinările criminalistice ale sistemelor de comunicații.</p>
-----------	--

Skills	<p>Până la sfârșitul cursului, studenții vor fi dezvoltat capacitatea de a aplica metode și instrumente criminalistice avansate pentru a investiga incidente care implică tehnologia informației și sistemele de comunicații. Vor fi capabili să colecteze, să păstreze și să analizeze sistematic dovezi digitale, asigurând respectarea standardelor legale și procedurale care mențin integritatea și admisibilitatea probelor în contexte judiciare sau organizaționale.</p> <p>Studenții vor dobândi abilități practice în efectuarea examinărilor criminalistice ale sistemelor informatice, rețelelor și platformelor de comunicații, inclusiv analiza sistemului de fișiere, inspecția traficului de rețea și recuperarea datelor șterse sau ascunse. Vor putea utiliza software și seturi de instrumente criminalistice specializate pentru a achiziționa imagini de disc, a analiza artefacte de sistem, a reconstrui cronologii și a identifica indicatori de compromitere.</p> <p>Prin exerciții practice și studii de caz, studenții vor învăța să analizeze comunicațiile digitale, cum ar fi e-mailurile, aplicațiile de mesagerie, VoIP și comunicațiile mobile, extragând metadata și conținut relevante pentru a sprijini investigațiile. Vor dezvolta capacitatea de a detecta, interpreta și documenta urme de încălcări de securitate, infracțiuni cibernetice sau încălcări ale politicilor, aplicând tehnici criminalistice adecvate în funcție de context.</p>
Responsibility and autonomy	<p>La finalizarea cursului, studenții vor fi capabili să lucreze independent și în colaborare pentru a planifica, desfășura și gestiona investigații criminalistice digitale în contexte tehnice și juridice complexe. Vor demonstra capacitatea de a-și asuma responsabilitatea pentru integritatea, acuratețea și legalitatea proceselor criminalistice, de la achiziția de probe până la analiză și raportare, asigurându-se că toate acțiunile respectă standardele etice, politicile organizaționale și cerințele legale.</p> <p>Studenții vor fi pregătiți să își asume roluri de conducere în echipe de investigație multidisciplinare, ghidând colegii și părțile interesate prin proceduri criminalistice, luarea deciziilor și raportare. Vor fi capabili să exercite o judecată profesională solidă atunci când gestionează date sensibile și iau decizii de investigație, inclusiv în situații care implică informații incomplete, tehnologii emergente sau tehnici anti-criminalistice avansate.</p> <p>Mai mult, studenții își vor dezvolta capacitatea de a reflecta critic asupra practicii lor profesionale, de a rămâne la curent cu metodele criminalistice digitale în evoluție și de a-și adapta continuu abordările pentru a face față noilor provocări din tehnologie și reglementare. Vor acționa cu un grad ridicat de responsabilitate și responsabilitate etică, recunoscând implicațiile juridice și societale mai largi ale investigațiilor criminalistice.</p>

8. Contents

8.1 Lecture	Teaching methods	Number of hours
1. Introducere în criminalitatea cibernetică / informatică: investigații privind securitatea informațiilor, criminologie informatică corporativă, metode științifice în analiza criminalistică, investigarea cazurilor de încălcări ale securității datelor. Analiza software-ului rău intenționat.	Prezentare Problematizare Conversație, interacțiune, argumentare sinteză	4
2. Tehnici criminalistice specializate; date ascunse și modalități de a le găsi, spyware și adware, metode de criptare și vulnerabilități. Protejarea datelor împotriva metodelor de urmărire pe internet, tehnologiilor wireless și sistemelor de securitate, sistemelor biometrice de securitate și securitatea acestora.	Metode care contribuie la dezvoltarea gândirii critice. Învățare independentă și cooperativă Generalizare	4

3. Hacking etic: terminologie esențială, hacking Windows, malware, scanare. Probe digitale în investigațiile penale: colectarea probelor, tipuri de probe, probe volatile, proceduri generale de colectare și arhivare a probelor, metode de colectare a probelor.	4
4. Identificarea datelor de interes: sincronizare, analiza dispozitivelor de supraveghere, reconstituirea evenimentelor anterioare, formatele de fișiere utilizate, conversia fișierelor, investigarea intruziunilor în rețea și a criminalității cibernetice, criminalistica rețelei și analiza jurnalelor. Investigarea traficului de rețea, investigarea atacurilor de internet, investigarea atacurilor asupra routerelor. Instrumente criminalistice și studii de caz.	2
Bibliography: <ul style="list-style-type: none"> [1]. Misra, Sanjay, and Chamundeswari Arumugam. <i>Illumination of Artificial Intelligence in Cybersecurity and Forensics</i>. Springer, 2022. [2]. Oettinger, William. <i>Learn Computer Forensics: Your One-Stop Guide to Searching, Analyzing, Acquiring, and Securing Digital Evidence</i>. Second edition, Packt Publishing Ltd., 2022. [3]. Kaushik, Keshav, et al., editors. <i>Advanced Smart Computing Technologies in Cybersecurity and Forensics</i>. First edition, CRC Press, 2022. [4]. Eoghan Casey, <i>Digital Evidence and Computer Crime Forensic science, Computers and Internet</i>, Elsevier Academic Press, 2011. [5]. Eoghan Casey (ed.), <i>Handbook of Digital Forensics and Investigation</i>, Academic Press. pp. 567, 2010. [6]. Eoghan Casey, <i>Computer Evidence and Computer Crime: Forensic Science, Computers, and the Internet</i>, Cambridge, Cambridge University Press, 2000. [7]. Vacca John R., <i>Computer Forensics Computer Crime Scene Investigation</i>, Massachusetts, Charles River Media, 2002. 	

8.2 Applications* (laboratory) <i>*The type is to be chosen according to the discipline</i>	Teaching methods	Number of hours
Investigații digitale: probe digitale și criminalitate cibernetică. Probe digitale în sala de judecată.	Metode interactive de predare-învățare Dialogul, Problematizarea, Conversația Metode active și interactive cu multiple metode care contribuie la dezvoltarea gândirii critice. Învățare independentă și cooperativă Sinteza / esențializarea informațiilor	4
Noțiuni de bază despre informatică pentru investigatorii digitali: Aplicarea științei criminalistice la computere - Examinarea criminalistică a sistemelor Windows, Examinarea criminalistică a sistemelor Unix		4
Rețele de calculatoare: introducere în rețelele de calculatoare pentru investigatorii digitali. Aplicarea științei criminalistice în rețelele de calculatoare: dovezi digitale pe nivelurile de rețea și transport; dovezi digitale pe Internet.		4
Investigarea criminalității cibernetice: investigarea intruziunilor		2
Bibliography:		

- [1]. Misra, Sanjay, and Chamundeswari Arumugam. *Illumination of Artificial Intelligence in Cybersecurity and Forensics*. Springer, 2022.
- [2]. Oettinger, William. *Learn Computer Forensics: Your One-Stop Guide to Searching, Analyzing, Acquiring, and Securing Digital Evidence*. Second edition, Packt Publishing Ltd., 2022.
- [3]. Kaushik, Keshav, et al., editors. *Advanced Smart Computing Technologies in Cybersecurity and Forensics*. First edition, CRC Press, 2022.
- [4]. Eoghan Casey, *Digital Evidence and Computer Crime Forensic science, Computers and Internet*, Elsevier Academic Press, 2011.
- [5]. Eoghan Casey (ed.), *Handbook of Digital Forensics and Investigation*, Academic Press. pp. 567, 2010.
- [6]. Eoghan Casey, *Computer Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Cambridge, Cambridge University Press, 2000.
- [7]. Vacca John R., *Computer Forensics Computer Crime Scene Investigation*, Massachusetts, Charles River Media, 2002.

9. Evaluation

Type of activity	9.1 Evaluation criteria	9.2 Evaluation methods	9.3 Percentage of final grade
9.4 Course			
9.5 Applications* (Seminar/Laboratory / Project) <i>*The type is to be chosen according to the discipline</i>	Aplicații de laborator, participare activă	Teste de laborator Proiect	50%
		Examination	50%
9.6 Minimum standard of achievement for the acquisition of the ECTS credits			
Prezentarea unui proiect și rezolvarea unei probleme date la examen. Nota 5/10			

Date of
completion
12.09.2025

Course Instructor,
Conf. Univ. Dr. Mihailescu Marius

Teaching Assistant,
Conf. Univ. Dr. Mihailescu Marius

Date of approval in the Department
19.09.2025

Head of Department
Conf. Univ. Dr. Pelican Elena

Dean,
Conf. Univ. Dr. Nicola Aurelian