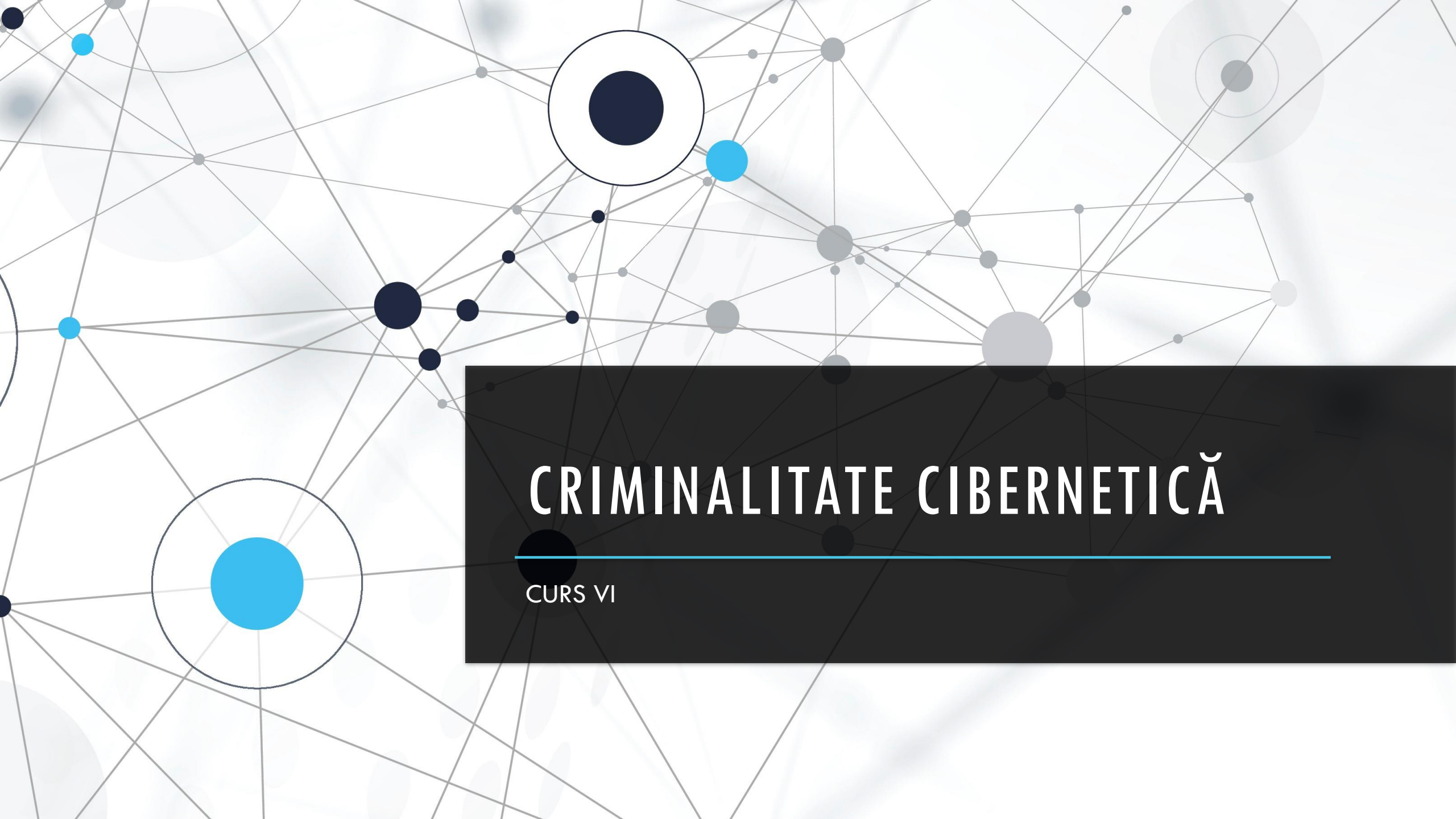

CRIMINALITATE CIBERNETICĂ

CURS VI

CRIMINALITATE CIBERNETICĂ INVESTIGAȚIA INFORMATICĂ

Elemente esențiale specifice investigațiilor informatice

Criminalistica informatică este procesul de detectare a atacurilor de hacking și de extragere corectă a dovezilor,menită să raporteze infracțiunea și să efectueze audituri pentru a preveni viitoarele atacuri

Criminalistica informatică permite identificarea sistematică și atentă a probelor digitale pentru cazuri de criminalitate și abuz conexe

Abilitățile necesare pentru a identifica urmele unui intrus și pentru colectarea în mod corespunzător a probelor necesare pentru urmărirea penală în instanța de judecată

INVESTIGAȚIA INFORMATICĂ

01: Fundamentele criminalisticii informatice

Fundamentele criminalisticii informatice

Dovezi digitale

Pregătire investigație

Rolurile și responsabilitățile unui investigator informatic

Conformitatea legală în criminalistica informatică

INVESTIGAȚIA INFORMATICĂ

02: Procesul de investigare a criminalisticii informatice

Procesul de investigare criminalistică și importanța acestuia

Procesul de investigare criminalistică - Faza de pre-investigare

Procesul de investigare criminalistică - Faza de investigare

Procesul de investigare criminalistică - Faza post-anchetă

INVESTIGAȚIA INFORMATICĂ

03: Înțelegerea hard disk-urilor și a sistemelor de fișiere

Diferite tipuri de unități de disc și caracteristicile lor

Structura logică a unui disc

Procesul de pornire a sistemelor de operare Windows, Linux și Mac

Sisteme de fișiere de sisteme de operare Windows, Linux și Mac

Examinarea sistemului de fișiere

INVESTIGAȚIA INFORMATICĂ

04: Achiziționarea și duplicarea datelor

Fundamentele achiziției de date

Tipuri de achiziție de date

Formatul achiziției de date

Metodologia achizitiei de date

INVESTIGAȚIA INFORMATICĂ

05: Depășirea tehnicilor anti-criminalistică

Anti-criminalistică și tehnicile sale

Contramăsuri anti-criminalistică

INVESTIGAȚIA INFORMATICĂ

06: Criminalistica Windows

Informații volatile și nevolatilate

Analiza memoriei Windows și a sistemului de registri

Cache, cookie-uri și istoric înregistrate în browserele web

Fișiere și metadate Windows

INVESTIGAȚIA INFORMATICĂ

07: Linux și Mac Criminalistică

Date volatile și nevolale în Linux

Analiza imaginilor sistemului de fișiere (utilizând kitul Sleuth)

Investigații criminalistice la nivel de memorie

Investigații Criminalistice specifice MacOS

INVESTIGAȚIA INFORMATICĂ

08: Investigații la nivel de rețea

Fundamentele criminalisticii de rețea

Concepte și tipuri de corelare a evenimentelor

Identificarea indicatorilor de compromis (IoCs) din jurnalele de rețea

Investigați traficul de rețea

INVESTIGAȚIA INFORMATICĂ

09: Investigarea atacurilor web

Criminalistica aplicațiilor Web

Sistemele de log-uri ale serverelor web IIS și Apache

Investigarea atacurilor web pe serverele bazate pe Windows

Detectare și investigare atacuri asupra aplicațiilor web

INVESTIGAȚIA INFORMATICĂ

10: Investigații Dark Web

Dark Web

Criminalitatea Dark Web

Tor Browser

INVESTIGAȚIA INFORMATICĂ

11: Investigarea infracțiunilor prin e-mail

Noțiuni de bază despre serviciul de rețea e-mail

Investigarea criminalității prin e-mail prin pași specifici

INVESTIGAȚIA INFORMATICĂ

12: Criminalistica malware

Malware, componente și metode de distribuție

Investigații malware și recunoașterea tipurilor de malware

Analiză malware

Analiza statică a malware-ului

Analiză documente Word suspecte

Analiza dinamică a malware-ului

Analiza comportamentului sistemului

Analiza comportamentului în rețea

INVESTIGAȚIA INFORMATICĂ

Bibliografie

EC-Council (International Council of Electronic Commerce Consultants), Digital Forensics Essentials (DFE), PROFESSIONAL SERIES, 2021