Teaching Schedule

040020309 – Cyber Security

Objective: To understand fundamentals of cyber security, be familiar with security attacks and security mechanisms, study legal perspectives of cyber security in India, gain knowledge of digital forensics and its usage in cyber security.

Course Outcomes: Upon completion of the course, students shall be able to

CO1: identify what cybercrime is and appreciate the importance of difference types cybercrime.
CO2: learn about different types of cybercriminals and the motives behind them.
CO3: illustrate various types of cyber attacks, tools used for gathering information about target.
CO4: examine a tools and methods used in cybercrime.
CO5: identify need for cyber laws, especially in the Indian context.
CO6:describe the meaning of digital signature, public-key infrastructure as well as the implications of digital signature in context of the Indian IT Act.
CO7:describe the fundamentals of digital forensics.
CO8: know about a tools and techniques for the forensics.

Unit	Sub Unit	No. of Lecture(s)	Topics	Reference Chapter/ Additional Reading	Teaching Methodologies	Evaluation Parameter
1.		**[05]**	**Cyber Security**			
	1.1, 1.2	1	Basic terminologies : Cybercrime, Cyber space, Cybersquatting, Cyber punk, Cyber warfare, Cyber fraud and cyber terrorism.	NGSB #1 Page no. 2 -3, 4	Presentation	**Seminar(Case Study Presentation)**
	1.3, 1.4	3	Cyber Criminals, Cyber crime classification	NGSB #1 Page no. 16 -19, 21-31	Presentation	
	1.5	1	Categories of cyber crime	NGSB #2 Page no. 46, 48 -49	Presentation	
2		**[07]**	**Cyber offenses**			
	2.1	1	Planning cyber attacks – phases, types and tools	NGSB #2 Page no. 49-50, 54, 58, 61	Discussion	**Quiz 1**
	2.2	1	Social engineering	NGSB #2 Page no. 61 – 65	Presentation	
	2.3	1	Cyber stalking : types and method	NGSB #2 Page no. 66-67	Discussion	
	2.4	1	Botnets	NGSB #2 Page no. 71-73	Presentation	

	2.5	1	Attack vectors	NGSB #2 Page no. 73-75	Discussion	
	2.6	1	Trends in mobility – types, classification of attacks in 3G mobile networks	NGSB #3 Page no. 84-86	Discussion	
	2.7	1	Credit Card frauds	NGSB #3 Page no. 87-90	Presentation	
3		**[06]**	**Cyber crime methods and security mechanisms**			
	3.1	1	Stages of a network attack	25NGSB #4 Page no. 125-126, 128	Presentation	**Unit Test 1**
	3.2	1	Denial Of Service attacks : Classification ,tools and preventive measures	NGSB #4 Page no. 158-161	Presentation	
	3.3	1	Distributed DOS attacks : Classification ,tools and preventive measures	NGSB #4 Page no. 162-164	Presentation	
	3.4	1	SQL injection : Agenda and prevention	NGSB #4 Page no. 164 -167	Video and Presentation	
	3.5	1	Buffer overflow: types and methods to minimize attacks	NGSB #4 Page no. 168-171	Presentation	
	3.6	1	Attacks on wireless networks – components of wireless networks, attack techniques and security mechanism	NGSB #4 Page no. 176--179	Presentation	
4		**[05]**	**Legal Perspectives of Cyber Security**			
	4.1	1	Indian ITA 2000 : ITA sections	NGSB #6 Page no. 254, 257 – 259	Conceptual reading from textbook	
	4.2	2	Digital signature and ITA: Public key certificate, PKI	NGSB #6 Page no. 273 - 274,276	Presentation	
	4.3	1	Representation of digital signatures in ITA 2000	NGSB #6 Page no. 274	Discussion	
	4.4	1	Cryptographic perspective of ITA 2000	NGSB #6 Page no. 279 -281	Discussion	

5		**[05]**	**Digital Forensics Fundamentals**			
	5.1	1	Digital forensics Science	NGSB #7 Page no. 320-321, 322	Presentation	**Unit Test 2**
	5.2	1	Cyber forensics and digital evidence	NGSB #7 Page no. 327, 331	Discussion	
	5.3	2	Digital forensics life cycle	NGSB #7 Page no. 339-347, 352	Presentation	
	5.4	1	Chain of custody concept	NGSB #7 Page no. 320-355-356	Presentation	
6		**[08]**	**Forensics Methods**			
	6.1	1	Relevance of OSI 7 layer model to computer forensics : OSI model overview, hacker agenda	NGSB #8 Page no. 373-376	Presentation	
	6.2	1	Special tools and techniques: Forensic toolkits	NGSB #8 Page no. 396 -399	Discussion	
	6.3	1	Data mining techniques used in forensics	NGSB #8 Page no. 402 -403	Presentation	
	6.4	3	Hand held devices and digital forensics	NGSB #8 Page no. 431, 433 – 453	Presentation	
	6.5	2	Tool kits for hand held devices	NGSB #8 Page no. 463 - 467	Presentation	
						Internal Exam

Text Book :

1. Nina Godbole , Sunit Belapure, Cyber Security – Understanding cyber crimes, computer forensics and legal perspectives, Wiley [NGSB]

Course Units and Course Outcomes Mapping

Unit No.	Unit	Course outcome							
		CO1	CO2	CO3	CO4	CO5	CO6	CO7	CO8
1	Cyber Security	✓	✓						
2	Cyberoffenses	✓	✓	✓					
3	Cyber crime methods and prevention	✓	✓		✓				
4	Legal Perspectives of Cyber Security			✓		✓	✓		
5	Digital Forensics fundamentals				✓			✓	✓
6	Forensics methods							✓	✓

Course Outcomes and Programme Outcomes Mapping

Course Outcomes	Programme Outcomes					
	PO1	PO2	PO3	PO4	PO5	PO6
CO1	✓			✓	✓	
CO2		✓		✓	✓	✓
CO3				✓	✓	✓
CO4				✓	✓	✓
CO5			✓	✓		
C06			✓	✓		
C07				✓	✓	✓
C08				✓	✓	✓

Activities/Practicum:

The following activities shall be carried out by the students.

- ❖ Self-study of following topics shall be done by the students:
  1. Key loggers and spywares.
  2. Virus and Worms.
  3. Trojan horse and backdoors.

The following activity shall be carried out by the course teacher

- ❖ Discuss real case studies of cyber stalking and harassment.
- ❖ Show demonstration of security settings at operating system and by security software .

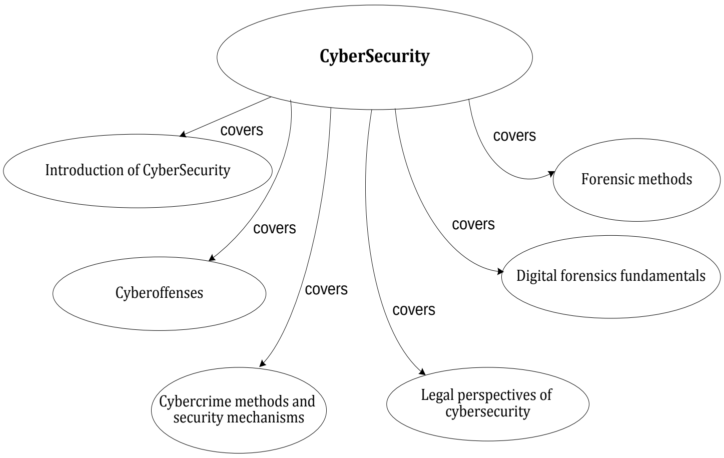
Modes of Transaction:

- ❖ For Unit 4: (All sub units), Students will bring their textbooks, I will make them underline important points and discuss them accordingly.
- ❖ Presentation and discussion will used as mode of transaction for rest of units.
- ❖ Video presentation will used for SQL injection attack and demonstration on Email Bombing.

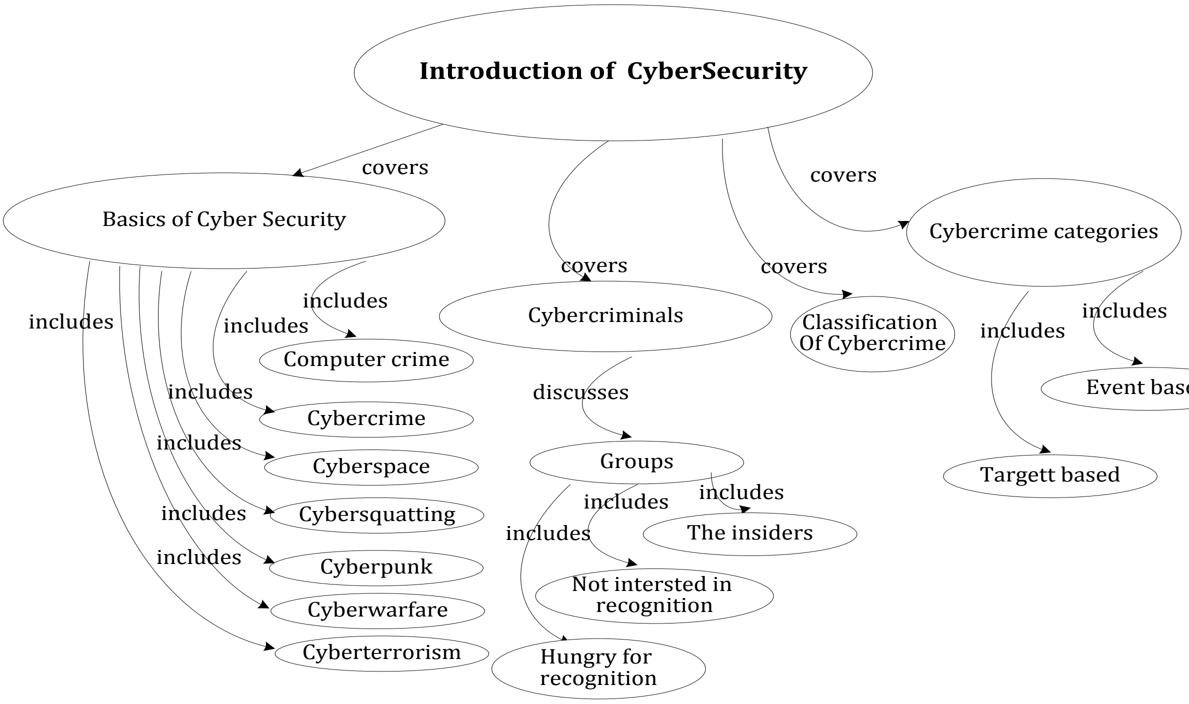
Concept Map:

It is a hierarchical / tree based representation of all topics covered under the course. This gives direct / indirect relationship /associations among topics as well as subtopics.

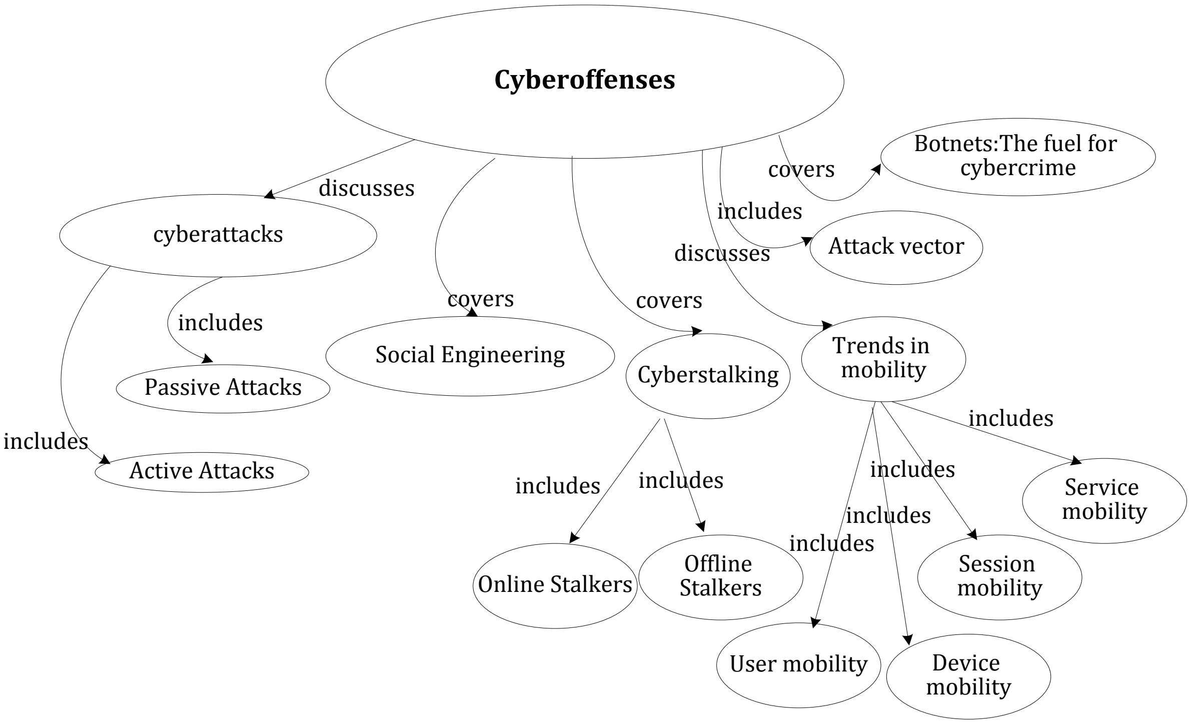
Course : Cyber Security


CyberSecurity
covers
Introduction of CyberSecurity
covers
Forensic methods
covers
Cyberoffenses
covers
Digital forensics fundamentals
covers
covers
Cybercrime methods and security mechanisms
Legal perspectives of cybersecurity

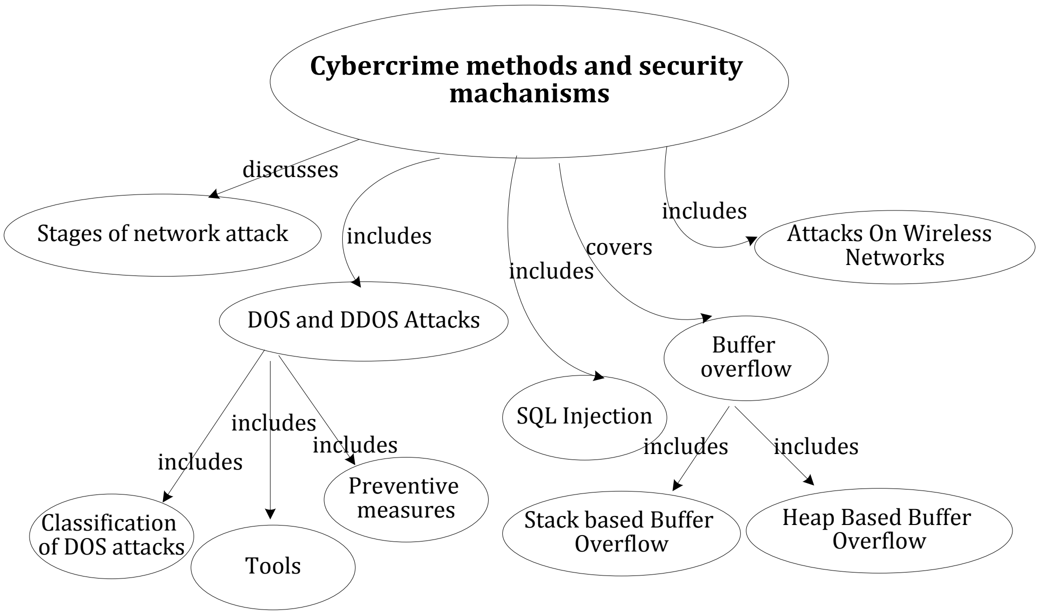
Unit 1: Cybersecurity



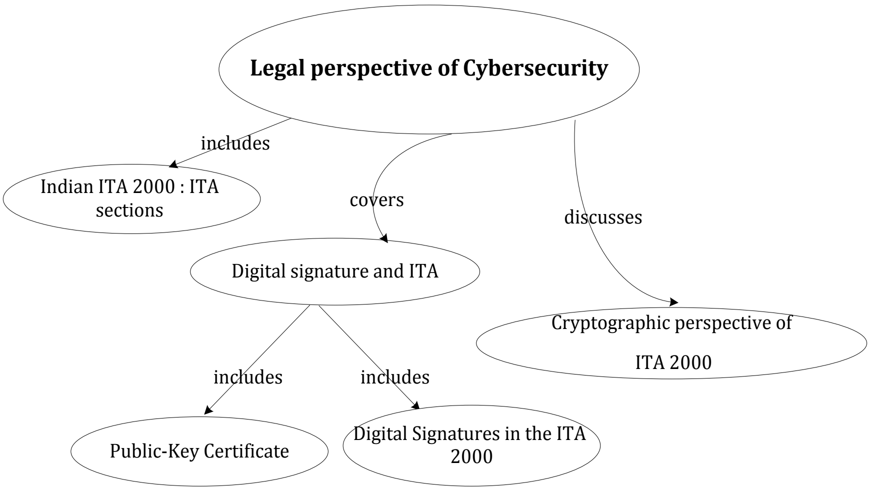
Unit 2: Cyberoffenses



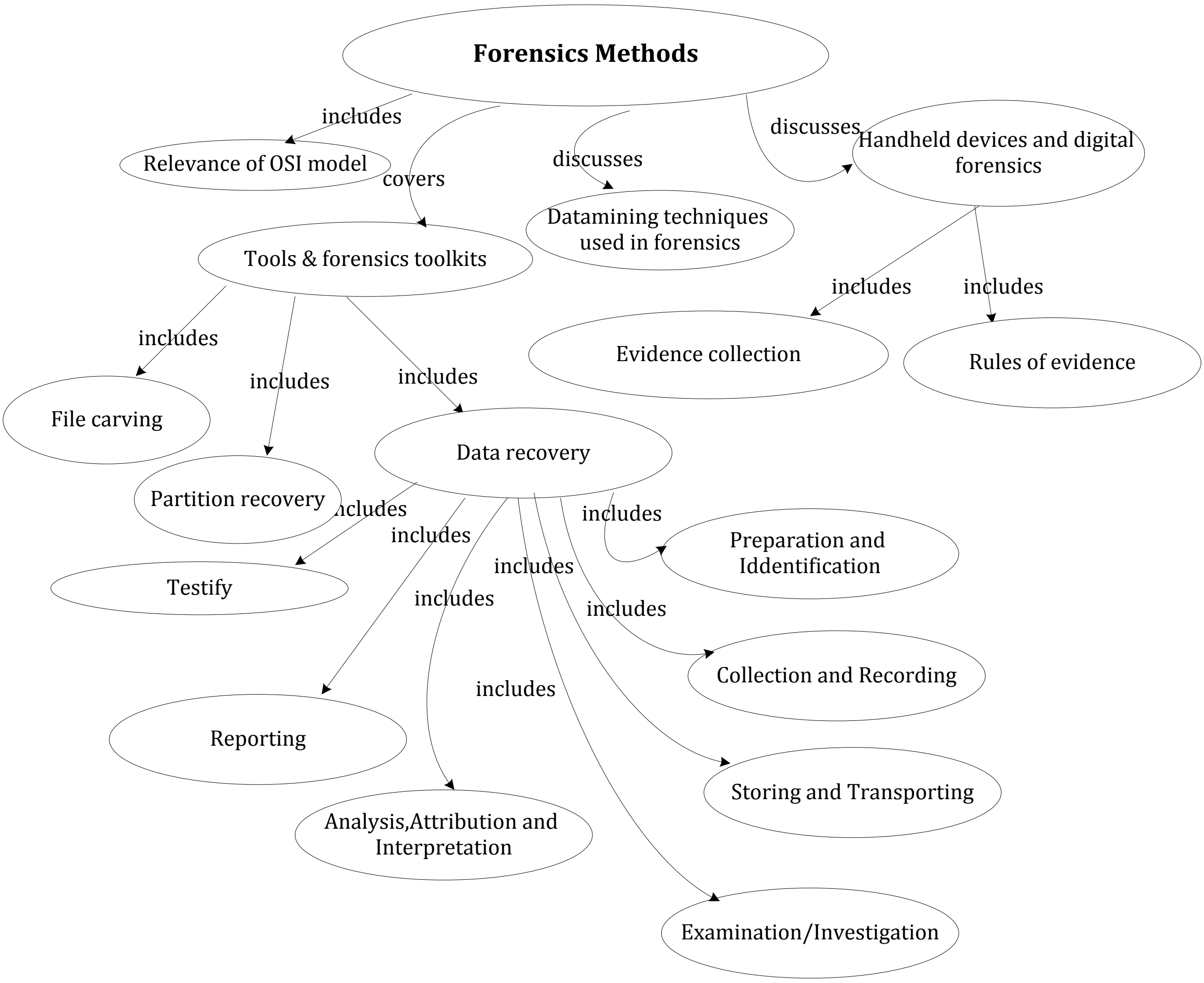
Unit 3: Cyber crime methods & security mechanisms



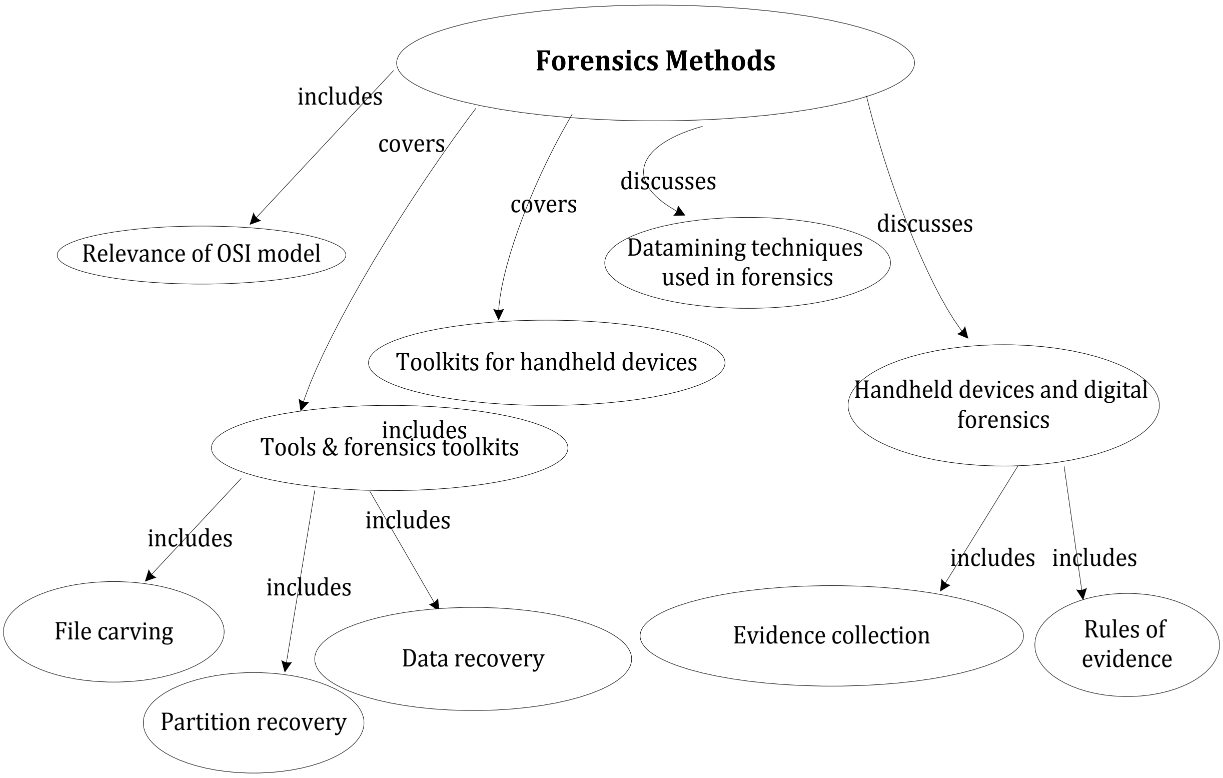
Unit 4: Legal perspective of cyber security


Legal perspective of Cybersecurity
includes
Indian ITA 2000 : ITA sections
covers
Digital signature and ITA
discusses
Cryptographic perspective of ITA 2000
includes
includes
Public-Key Certificate
Digital Signatures in the ITA 2000

Unit 5: Digital forensics fundamentals



Unit 6: Forensics methods


Forensics Methods
includes
covers
covers
discusses
discusses
Relevance of OSI model
Datamining techniques used in forensics
Toolkits for handheld devices
Handheld devices and digital forensics
includes
Tools & forensics toolkits
includes
includes
includes
includes
includes
File carving
Data recovery
Evidence collection
Rules of evidence
Partition recovery