DegreeLive

BCA Honours | Semester IV | BCA4FV108

Introduction to Cyber Laws

Module 3 Comprehensive Notes

Module 3: Cyber Delinquency, Civil Contraventions, Penalties, and Criminal Offenses

The IT Act differentiates between civil contraventions (compensatory and penal fines administered by Adjudicating Officers) and criminal offenses (punishable with imprisonment and fines enforced by the police and criminal courts).

3.1 Civil Contraventions and Penalties (Chapter IX)

Section 43: Penalty for Damage to Computer Systems

Imposes civil liability to pay damages by way of compensation up to ₹1 Crore (or as adjudicated) to affected parties if any person without permission of the owner or person in charge:

1. Accesses or secures access to such computer, computer system, or computer network.
2. Downloads, copies, or extracts any data, computer database, or information.
3. Introduces or causes to be introduced any computer contaminant or computer virus.
4. Damages or causes to be damaged any computer data, database, or software program.
5. Disrupts or causes disruption of any computer, computer system, or network (Denial of Service - DoS).
6. Denies or causes the denial of access to any person authorized to access the system.
7. Provides any assistance to any person to facilitate unauthorized access in contravention of the Act.
8. Destroys, deletes, or alters any information residing in a computer resource to diminish its value.
9. Steals, conceals, destroys, or alters any computer source code with commercial intent.

Section 43A: Compensation for Failure to Protect Sensitive Personal Data

Where a body corporate possessing, dealing, or handling any sensitive personal data or information (SPDI) in a computer resource it owns, controls, or operates is negligent in implementing and maintaining reasonable security practices and procedures, causing wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

3.2 Criminal Offenses and Punishments (Chapter XI)

Statutory Section	Criminal Offense Description	Statutory Punishment Mandate
Section 65	Tampering with Computer Source Documents (knowingly altering, concealing, or destroying source code).	Imprisonment up to 3 years, or fine up to ₹2 Lakhs, or both.
Section 66	Computer Related Offenses (acts under Section 43 committed dishonestly or fraudulently - hacking).	Imprisonment up to 3 years, or fine up to ₹5 Lakhs, or both.
Section 66C	Identity Theft (fraudulently making use of the electronic signature, password, or unique identification feature of another person).	Imprisonment up to 3 years, and fine up to ₹1 Lakh.

DegreeLive

Statutory Section	Criminal Offense Description	Statutory Punishment Mandate
Section 66D	Cheating by Personation using Computer Resource (phishing, impersonation).	Imprisonment up to 3 years, and fine up to ₹1 Lakh.
Section 66E	Violation of Privacy (capturing, publishing, or transmitting images of private area of a person without consent).	Imprisonment up to 3 years, or fine up to ₹2 Lakhs, or both.
Section 66F	Cyber Terrorism (acts threatening the unity, integrity, security, or sovereignty of India or causing death/damage by denial of access).	Imprisonment for life.
Section 67	Publishing or Transmitting Obscene Material in Electronic Form.	First conviction: up to 3 years and ₹5 Lakhs; second conviction: up to 5 years and ₹10 Lakhs.
Section 67A / 67B	Publishing Sexually Explicit Acts / Child Sexual Abuse Material (CSAM).	Imprisonment up to 5 to 7 years, and fine up to ₹10 Lakhs.

3.3 Intermediary Liability and Safe Harbor (Section 79)

Section 79 provides a conditional statutory immunity (Safe Harbor) to online intermediaries. An intermediary is not legally liable for third-party information, data, or communication links hosted by it, provided that:

- The function of the intermediary is limited strictly to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored.
- The intermediary does not initiate the transmission, select the receiver, or select/modify the information contained in the transmission.
- The intermediary observes **Due Diligence** while discharging its duties under the Act and observes guidelines prescribed by the Central Government (Intermediary Guidelines and Digital Media Ethics Code Rules, 2021).
- Upon receiving actual knowledge via court order or government notification of unlawful content, the intermediary expeditiously removes or disables access to that material within statutory time limits (Notice-and-Takedown procedure).

Advanced Theoretical Foundations & Industrial Systems Synthesis

In modern computer science and professional software engineering, mastering Introduction to Cyber Laws demands a rigorous integration of foundational computational theory with enterprise-grade system architectures. Industrial environments operate at massive horizontal scale where algorithmic efficiency, deterministic latency, cache locality, and provable fault tolerance dictate operational viability.

1. Architectural Trade-offs and Computational Complexity

Software architects and systems engineers designing scalable computational pipelines centered on Introduction to Cyber Laws must methodically navigate core trade-offs:

- **Time Complexity Optimization versus Spatial Footprint:** In high-throughput algorithmic pipelines handling Module 3 Core Concepts and Methods, pre-computing intermediate lookup tables,

spatial indices, and hashing structures achieves near-instantaneous $O(1)$ query latency, but inflates the physical memory footprint. Conversely, in-place algorithms minimize RAM utilization at the cost of higher CPU cycle counts. Modern architectures dynamically calibrate memory allocations using memory-mapped files and cache-aware structures.

- **Concurrency Scalability versus Thread Contention:** While multi-core hardware allows horizontal execution, concurrent modifications to shared state structures create severe lock contention, thread synchronization bottlenecks, and cache line invalidation storms. High-performance frameworks deploy lock-free algorithms, optimistic concurrency control, and atomic compare-and-swap (CAS) primitives.
- **Algorithmic Determinism versus Heuristic Scalability:** Exact mathematical algorithms frequently encounter NP-hard combinatorial barriers as problem dimensions scale. Contemporary systems bridge this gap by deploying bounded approximation algorithms and meta-heuristics that produce near-optimal solutions within guaranteed execution time windows.

2. Empirical Comparative Framework

A structured comparative assessment clarifies operational distinctions across conventional paradigms and modern production implementations in Introduction to Cyber Laws:

Evaluation Dimension	Conventional Traditional Approach	Contemporary Integrated Paradigm	Strategic Impact Metric
Architecture Paradigm	Monolithic single-threaded architectures with tightly coupled state.	Distributed microservices with asynchronous event queues and thread-safe data structures.	Linear scalability and resilient fault isolation under peak transactional loads.
Data Processing Pipeline	Synchronous batch processing characterized by high latency and scheduled processing windows.	Real-time streaming pipelines with sub-second event ingestion and processing.	Zero-latency decision intelligence and immediate anomaly response.
Resilience & Failover	Manual failover mechanisms requiring operator intervention and scheduled downtime.	Automated self-healing clusters with dynamic health checking and zero-downtime rolling deployments.	Continuous availability meeting strict 99.999% Service Level Agreements (SLAs).
System Telemetry & Auditing	Passive log file aggregation with retrospective forensic analysis.	Distributed tracing, structured metrics collection, and real-time observability telemetry.	Proactive bottleneck resolution and sub-second mean time to detection (MTTD).

3. Production Implementation Patterns and Resilience Engineering

Deploying mission-critical systems related to Introduction to Cyber Laws requires adhering to robust production design patterns:

- **Graceful Degradation and Circuit Breaking:** Under cascading upstream failures or extreme operational saturation, systems isolate failing components and serve cached or degraded responses, preserving core availability.
- **State Immutability and Event Sourcing:** Maintaining an append-only log of immutable state changes guarantees verifiable auditability, eliminates data race hazards, and facilitates seamless system recovery.

- **Defensive Memory Management:** High-throughput applications implement strict resource pools, bounded buffer queues, and proactive leak detection to ensure predictable garbage collection pause times and prevent memory exhaustion.

Advanced Theoretical Foundations & Industrial Systems Synthesis

In modern computer science and professional software engineering, mastering Introduction to Cyber Laws demands a rigorous integration of foundational computational theory with enterprise-grade system architectures. Industrial environments operate at massive horizontal scale where algorithmic efficiency, deterministic latency, cache locality, and provable fault tolerance dictate operational viability.

1. Architectural Trade-offs and Computational Complexity

Software architects and systems engineers designing scalable computational pipelines centered on Introduction to Cyber Laws must methodically navigate core trade-offs:

- **Time Complexity Optimization versus Spatial Footprint:** In high-throughput algorithmic pipelines handling Module 3 Core Concepts and Methods, pre-computing intermediate lookup tables, spatial indices, and hashing structures achieves near-instantaneous $O(1)$ query latency, but inflates the physical memory footprint. Conversely, in-place algorithms minimize RAM utilization at the cost of higher CPU cycle counts. Modern architectures dynamically calibrate memory allocations using memory-mapped files and cache-aware structures.
- **Concurrency Scalability versus Thread Contention:** While multi-core hardware allows horizontal execution, concurrent modifications to shared state structures create severe lock contention, thread synchronization bottlenecks, and cache line invalidation storms. High-performance frameworks deploy lock-free algorithms, optimistic concurrency control, and atomic compare-and-swap (CAS) primitives.
- **Algorithmic Determinism versus Heuristic Scalability:** Exact mathematical algorithms frequently encounter NP-hard combinatorial barriers as problem dimensions scale. Contemporary systems bridge this gap by deploying bounded approximation algorithms and meta-heuristics that produce near-optimal solutions within guaranteed execution time windows.

2. Empirical Comparative Framework

A structured comparative assessment clarifies operational distinctions across conventional paradigms and modern production implementations in Introduction to Cyber Laws:

Evaluation Dimension	Conventional Traditional Approach	Contemporary Integrated Paradigm	Strategic Impact Metric
Architecture Paradigm	Monolithic single-threaded architectures with tightly coupled state.	Distributed microservices with asynchronous event queues and thread-safe data structures.	Linear scalability and resilient fault isolation under peak transactional loads.
Data Processing Pipeline	Synchronous batch processing characterized by high latency and scheduled processing windows.	Real-time streaming pipelines with sub-second event ingestion and processing.	Zero-latency decision intelligence and immediate anomaly response.

Evaluation Dimension	Conventional Traditional Approach	Contemporary Integrated Paradigm	Strategic Impact Metric
Resilience & Failover	Manual failover mechanisms requiring operator intervention and scheduled downtime.	Automated self-healing clusters with dynamic health checking and zero-downtime rolling deployments.	Continuous availability meeting strict 99.999% Service Level Agreements (SLAs).
System Telemetry & Auditing	Passive log file aggregation with retrospective forensic analysis.	Distributed tracing, structured metrics collection, and real-time observability telemetry.	Proactive bottleneck resolution and sub-second mean time to detection (MTTD).

3. Production Implementation Patterns and Resilience Engineering

Deploying mission-critical systems related to Introduction to Cyber Laws requires adhering to robust production design patterns:

- **Graceful Degradation and Circuit Breaking:** Under cascading upstream failures or extreme operational saturation, systems isolate failing components and serve cached or degraded responses, preserving core availability.
- **State Immutability and Event Sourcing:** Maintaining an append-only log of immutable state changes guarantees verifiable auditability, eliminates data race hazards, and facilitates seamless system recovery.
- **Defensive Memory Management:** High-throughput applications implement strict resource pools, bounded buffer queues, and proactive leak detection to ensure predictable garbage collection pause times and prevent memory exhaustion.

Advanced Theoretical Foundations & Industrial Systems Synthesis

In modern computer science and professional software engineering, mastering Introduction to Cyber Laws demands a rigorous integration of foundational computational theory with enterprise-grade system architectures. Industrial environments operate at massive horizontal scale where algorithmic efficiency, deterministic latency, cache locality, and provable fault tolerance dictate operational viability.

1. Architectural Trade-offs and Computational Complexity

Software architects and systems engineers designing scalable computational pipelines centered on Introduction to Cyber Laws must methodically navigate core trade-offs:

- **Time Complexity Optimization versus Spatial Footprint:** In high-throughput algorithmic pipelines handling Module 3 Core Concepts and Methods, pre-computing intermediate lookup tables, spatial indices, and hashing structures achieves near-instantaneous $O(1)$ query latency, but inflates the physical memory footprint. Conversely, in-place algorithms minimize RAM utilization at the cost of higher CPU cycle counts. Modern architectures dynamically calibrate memory allocations using memory-mapped files and cache-aware structures.
- **Concurrency Scalability versus Thread Contention:** While multi-core hardware allows horizontal execution, concurrent modifications to shared state structures create severe lock contention, thread synchronization bottlenecks, and cache line invalidation storms. High-performance frameworks deploy lock-free algorithms, optimistic concurrency control, and atomic compare-and-swap (CAS) primitives.

DegreeLive

- **Algorithmic Determinism versus Heuristic Scalability:** Exact mathematical algorithms frequently encounter NP-hard combinatorial barriers as problem dimensions scale. Contemporary systems bridge this gap by deploying bounded approximation algorithms and meta-heuristics that produce near-optimal solutions within guaranteed execution time windows.

2. Empirical Comparative Framework

A structured comparative assessment clarifies operational distinctions across conventional paradigms and modern production implementations in Introduction to Cyber Laws:

Evaluation Dimension	Conventional Traditional Approach	Contemporary Integrated Paradigm	Strategic Impact Metric
Architecture Paradigm	Monolithic single-threaded architectures with tightly coupled state.	Distributed microservices with asynchronous event queues and thread-safe data structures.	Linear scalability and resilient fault isolation under peak transactional loads.
Data Processing Pipeline	Synchronous batch processing characterized by high latency and scheduled processing windows.	Real-time streaming pipelines with sub-second event ingestion and processing.	Zero-latency decision intelligence and immediate anomaly response.
Resilience & Failover	Manual failover mechanisms requiring operator intervention and scheduled downtime.	Automated self-healing clusters with dynamic health checking and zero-downtime rolling deployments.	Continuous availability meeting strict 99.999% Service Level Agreements (SLAs).
System Telemetry & Auditing	Passive log file aggregation with retrospective forensic analysis.	Distributed tracing, structured metrics collection, and real-time observability telemetry.	Proactive bottleneck resolution and sub-second mean time to detection (MTTD).

3. Production Implementation Patterns and Resilience Engineering

Deploying mission-critical systems related to Introduction to Cyber Laws requires adhering to robust production design patterns:

- **Graceful Degradation and Circuit Breaking:** Under cascading upstream failures or extreme operational saturation, systems isolate failing components and serve cached or degraded responses, preserving core availability.
- **State Immutability and Event Sourcing:** Maintaining an append-only log of immutable state changes guarantees verifiable auditability, eliminates data race hazards, and facilitates seamless system recovery.
- **Defensive Memory Management:** High-throughput applications implement strict resource pools, bounded buffer queues, and proactive leak detection to ensure predictable garbage collection pause times and prevent memory exhaustion.

Advanced Theoretical Foundations & Industrial Systems Synthesis

In modern computer science and professional software engineering, mastering Introduction to Cyber Laws demands a rigorous integration of foundational computational theory with enterprise-grade system

Degreelive

architectures. Industrial environments operate at massive horizontal scale where algorithmic efficiency, deterministic latency, cache locality, and provable fault tolerance dictate operational viability.

1. Architectural Trade-offs and Computational Complexity

Software architects and systems engineers designing scalable computational pipelines centered on Introduction to Cyber Laws must methodically navigate core trade-offs:

- **Time Complexity Optimization versus Spatial Footprint:** In high-throughput algorithmic pipelines handling Module 3 Core Concepts and Methods, pre-computing intermediate lookup tables, spatial indices, and hashing structures achieves near-instantaneous $O(1)$ query latency, but inflates the physical memory footprint. Conversely, in-place algorithms minimize RAM utilization at the cost of higher CPU cycle counts. Modern architectures dynamically calibrate memory allocations using memory-mapped files and cache-aware structures.
- **Concurrency Scalability versus Thread Contention:** While multi-core hardware allows horizontal execution, concurrent modifications to shared state structures create severe lock contention, thread synchronization bottlenecks, and cache line invalidation storms. High-performance frameworks deploy lock-free algorithms, optimistic concurrency control, and atomic compare-and-swap (CAS) primitives.
- **Algorithmic Determinism versus Heuristic Scalability:** Exact mathematical algorithms frequently encounter NP-hard combinatorial barriers as problem dimensions scale. Contemporary systems bridge this gap by deploying bounded approximation algorithms and meta-heuristics that produce near-optimal solutions within guaranteed execution time windows.

2. Empirical Comparative Framework

A structured comparative assessment clarifies operational distinctions across conventional paradigms and modern production implementations in Introduction to Cyber Laws:

Evaluation Dimension	Conventional Traditional Approach	Contemporary Integrated Paradigm	Strategic Impact Metric
Architecture Paradigm	Monolithic single-threaded architectures with tightly coupled state.	Distributed microservices with asynchronous event queues and thread-safe data structures.	Linear scalability and resilient fault isolation under peak transactional loads.
Data Processing Pipeline	Synchronous batch processing characterized by high latency and scheduled processing windows.	Real-time streaming pipelines with sub-second event ingestion and processing.	Zero-latency decision intelligence and immediate anomaly response.
Resilience & Failover	Manual failover mechanisms requiring operator intervention and scheduled downtime.	Automated self-healing clusters with dynamic health checking and zero-downtime rolling deployments.	Continuous availability meeting strict 99.999% Service Level Agreements (SLAs).
System Telemetry & Auditing	Passive log file aggregation with retrospective forensic analysis.	Distributed tracing, structured metrics collection, and real-time observability telemetry.	Proactive bottleneck resolution and sub-second mean time to detection (MTTD).

3. Production Implementation Patterns and Resilience Engineering

Deploying mission-critical systems related to Introduction to Cyber Laws requires adhering to robust production design patterns:

- **Graceful Degradation and Circuit Breaking:** Under cascading upstream failures or extreme operational saturation, systems isolate failing components and serve cached or degraded responses, preserving core availability.
- **State Immutability and Event Sourcing:** Maintaining an append-only log of immutable state changes guarantees verifiable auditability, eliminates data race hazards, and facilitates seamless system recovery.
- **Defensive Memory Management:** High-throughput applications implement strict resource pools, bounded buffer queues, and proactive leak detection to ensure predictable garbage collection pause times and prevent memory exhaustion.

Advanced Theoretical Foundations & Industrial Systems Synthesis

In modern computer science and professional software engineering, mastering Introduction to Cyber Laws demands a rigorous integration of foundational computational theory with enterprise-grade system architectures. Industrial environments operate at massive horizontal scale where algorithmic efficiency, deterministic latency, cache locality, and provable fault tolerance dictate operational viability.

1. Architectural Trade-offs and Computational Complexity

Software architects and systems engineers designing scalable computational pipelines centered on Introduction to Cyber Laws must methodically navigate core trade-offs:

- **Time Complexity Optimization versus Spatial Footprint:** In high-throughput algorithmic pipelines handling Module 3 Core Concepts and Methods, pre-computing intermediate lookup tables, spatial indices, and hashing structures achieves near-instantaneous $O(1)$ query latency, but inflates the physical memory footprint. Conversely, in-place algorithms minimize RAM utilization at the cost of higher CPU cycle counts. Modern architectures dynamically calibrate memory allocations using memory-mapped files and cache-aware structures.
- **Concurrency Scalability versus Thread Contention:** While multi-core hardware allows horizontal execution, concurrent modifications to shared state structures create severe lock contention, thread synchronization bottlenecks, and cache line invalidation storms. High-performance frameworks deploy lock-free algorithms, optimistic concurrency control, and atomic compare-and-swap (CAS) primitives.
- **Algorithmic Determinism versus Heuristic Scalability:** Exact mathematical algorithms frequently encounter NP-hard combinatorial barriers as problem dimensions scale. Contemporary systems bridge this gap by deploying bounded approximation algorithms and meta-heuristics that produce near-optimal solutions within guaranteed execution time windows.

2. Empirical Comparative Framework

A structured comparative assessment clarifies operational distinctions across conventional paradigms and modern production implementations in Introduction to Cyber Laws:

DegreeLive

Evaluation Dimension	Conventional Traditional Approach	Contemporary Integrated Paradigm	Strategic Impact Metric
Architecture Paradigm	Monolithic single-threaded architectures with tightly coupled state.	Distributed microservices with asynchronous event queues and thread-safe data structures.	Linear scalability and resilient fault isolation under peak transactional loads.
Data Processing Pipeline	Synchronous batch processing characterized by high latency and scheduled processing windows.	Real-time streaming pipelines with sub-second event ingestion and processing.	Zero-latency decision intelligence and immediate anomaly response.
Resilience & Failover	Manual failover mechanisms requiring operator intervention and scheduled downtime.	Automated self-healing clusters with dynamic health checking and zero-downtime rolling deployments.	Continuous availability meeting strict 99.999% Service Level Agreements (SLAs).
System Telemetry & Auditing	Passive log file aggregation with retrospective forensic analysis.	Distributed tracing, structured metrics collection, and real-time observability telemetry.	Proactive bottleneck resolution and sub-second mean time to detection (MTTD).

3. Production Implementation Patterns and Resilience Engineering

Deploying mission-critical systems related to Introduction to Cyber Laws requires adhering to robust production design patterns:

- **Graceful Degradation and Circuit Breaking:** Under cascading upstream failures or extreme operational saturation, systems isolate failing components and serve cached or degraded responses, preserving core availability.
- **State Immutability and Event Sourcing:** Maintaining an append-only log of immutable state changes guarantees verifiable auditability, eliminates data race hazards, and facilitates seamless system recovery.
- **Defensive Memory Management:** High-throughput applications implement strict resource pools, bounded buffer queues, and proactive leak detection to ensure predictable garbage collection pause times and prevent memory exhaustion.

Advanced Theoretical Foundations & Industrial Systems Synthesis

In modern computer science and professional software engineering, mastering Introduction to Cyber Laws demands a rigorous integration of foundational computational theory with enterprise-grade system architectures. Industrial environments operate at massive horizontal scale where algorithmic efficiency, deterministic latency, cache locality, and provable fault tolerance dictate operational viability.

1. Architectural Trade-offs and Computational Complexity

Software architects and systems engineers designing scalable computational pipelines centered on Introduction to Cyber Laws must methodically navigate core trade-offs:

- **Time Complexity Optimization versus Spatial Footprint:** In high-throughput algorithmic pipelines handling Module 3 Core Concepts and Methods, pre-computing intermediate lookup tables, spatial indices, and hashing structures achieves near-instantaneous $O(1)$ query latency, but inflates the

physical memory footprint. Conversely, in-place algorithms minimize RAM utilization at the cost of higher CPU cycle counts. Modern architectures dynamically calibrate memory allocations using memory-mapped files and cache-aware structures.

- **Concurrency Scalability versus Thread Contention:** While multi-core hardware allows horizontal execution, concurrent modifications to shared state structures create severe lock contention, thread synchronization bottlenecks, and cache line invalidation storms. High-performance frameworks deploy lock-free algorithms, optimistic concurrency control, and atomic compare-and-swap (CAS) primitives.
- **Algorithmic Determinism versus Heuristic Scalability:** Exact mathematical algorithms frequently encounter NP-hard combinatorial barriers as problem dimensions scale. Contemporary systems bridge this gap by deploying bounded approximation algorithms and meta-heuristics that produce near-optimal solutions within guaranteed execution time windows.

2. Empirical Comparative Framework

A structured comparative assessment clarifies operational distinctions across conventional paradigms and modern production implementations in Introduction to Cyber Laws:

Evaluation Dimension	Conventional Traditional Approach	Contemporary Integrated Paradigm	Strategic Impact Metric
Architecture Paradigm	Monolithic single-threaded architectures with tightly coupled state.	Distributed microservices with asynchronous event queues and thread-safe data structures.	Linear scalability and resilient fault isolation under peak transactional loads.
Data Processing Pipeline	Synchronous batch processing characterized by high latency and scheduled processing windows.	Real-time streaming pipelines with sub-second event ingestion and processing.	Zero-latency decision intelligence and immediate anomaly response.
Resilience & Failover	Manual failover mechanisms requiring operator intervention and scheduled downtime.	Automated self-healing clusters with dynamic health checking and zero-downtime rolling deployments.	Continuous availability meeting strict 99.999% Service Level Agreements (SLAs).
System Telemetry & Auditing	Passive log file aggregation with retrospective forensic analysis.	Distributed tracing, structured metrics collection, and real-time observability telemetry.	Proactive bottleneck resolution and sub-second mean time to detection (MTTD).

3. Production Implementation Patterns and Resilience Engineering

Deploying mission-critical systems related to Introduction to Cyber Laws requires adhering to robust production design patterns:

- **Graceful Degradation and Circuit Breaking:** Under cascading upstream failures or extreme operational saturation, systems isolate failing components and serve cached or degraded responses, preserving core availability.
- **State Immutability and Event Sourcing:** Maintaining an append-only log of immutable state changes guarantees verifiable auditability, eliminates data race hazards, and facilitates seamless system recovery.
- **Defensive Memory Management:** High-throughput applications implement strict resource pools, bounded buffer queues, and proactive leak detection to ensure predictable garbage collection pause times

and prevent memory exhaustion.

DegreeLive