Towards efficient automation of digital crime investigation using Reinforcement Learning (RL)

Dr Mohamed Chahine GHANEM
My Background

- Engineering Degree, MSc (Dist.) in Digital Forensics and PhD in Cyber Security form City, University of London

- Fellow of Higher Education Academy (FHEA)

- Deputy-Director of the Cyber Security Research Centre (applied-research in the domain of digital forensics, cyber-security, computing and AI).

- Principal Lecturer in Digital Forensics and Cyber-security (BSc course leader)

- DFIR expert (few Certifications such as CISSP, CEH, GCFE, EnCE, ACE, XRY and CPCI) with 10+ years of corporate and law-enforcement experience in digital-crime investigation and offensive cyber-security

- Founding head of Londonmet Digital Forensics Laboratory (RKE to provide Digital forensic investigations services in civil and criminal cases for law firms, businesses and private clients in UK, and Internship form our students)
What is digital forensic?

Digital Forensics is the use of scientifically derived and proven methods toward:

- the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital devices.

- for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.
Branches of Digital Forensics

• The technical aspect of an investigation is divided into several sub-branches, relating to the type of digital devices involved:
  ✓ Computer forensics, Firewall Forensics, Database Forensics, Network forensics, Forensic data analysis and Mobile device forensics.

• The typical forensic process encompasses the seizure, forensic imaging and analysis of digital media and the production of a report into collected evidence.
Example of digital devices and contained evidences

- e-mails,
- digital photographs,
- ATM transaction logs,
- word processing documents,
- Instant message histories,
- files saved from accounting program,
- spreadsheets,
- internet browser histories,
- databases,
- the contents of computer memory,
- computer backups, computer printouts,
- Global Positioning System tracks,
- logs from a hotel’s electronic door locks, and
- digital video or audio files
Digital Evidence

Evidence
A piece of information that supports a conclusion

Digital evidence
Any data that is recorded or preserved on any medium in or by a computer system or other similar digital device, that can be read or understood by a person or a computer system or other similar device.

It includes a display, printout or other output of that data.
Digital Forensic Process

✓ Identification
✓ Preservation
✓ Analysis
✓ Documentation
✓ Presentation

[Diagram showing the digital forensic process with steps such as media collection, data examination, information analysis, and evidences obtained results.]
Skills required for Digital Forensics

- Application of Programming or computer-related experience
- Broad understanding of operating systems and applications
- Strong analytical skills
- Strong computer science fundamentals
- Strong system administrative skills
- Knowledge of the latest intruder tools
- Knowledge of cryptography and steganography
- Strong understanding of the rules of evidence and evidence handling
- Ability to be an expert witness in a court of law
Types of Digital Evidence

**Persistant data**

Meaning data that *remains intact* when the digital device is turned off. E.g. hard drives, disk drives and removable storage devices (such as USB drives or flash drives).

**Volatile data**

Which is data that *would be lost* if the digital device is turned off. E.g. deleted files, computer history, the computers registry, temporary files and web browsing history.
Challenges in DFIR

- **Explosion of complexity**: evidence is no longer confined within a single host but, rather, is scattered among different physical or virtual locations.

- **Development of standards**: No standard formats, schema, and ontologies

- **Privacy-preserving investigations**: people bring into cyberspace many aspects of their lives, primarily through online social networks or social media sites. Other hurdles when cloud computing is involved.

- **Legitimacy**: modern infrastructures are becoming complex and virtualized, often shifting their complexity at the border or delegating some duties to third parties

- **Rise of Anti-forensics techniques**: defensive measures encompass encryption, obfuscation, and cloaking techniques, including information hiding.
Limits of Current Human-led DFIR practice

Volume of Evidence
High level of complexity
Usage of security and anti-forensics

Expertise of Investigator
Time constraint
Investigative Lead

Device subject to investigation

Evidence

Hypothetical 'line of sight' barrier

'Insight' created by available case intelligence or manual review.

Filetype / search / location 1
Filetype / search / location 2
Filetype / search / location n
The four Vs challenges in DFIR

The four main challenges that big data bought into Digital Forensics are:

**Volume** is often used to reference the amount of data collected from an individual or multiple seized devices.

**Variety** to reference the different types of files or data present within the medium (for example this could be allocated data from known file systems and unallocated data from volume and file slack spaces).

**Velocity** is concerned with the amount of time needed to process and analyse the acquired data and indeed the time often needed to acquire the data initially.

**Value** of the data. this is not the resale value, but the value of the actual intelligence collected when the data is processed correctly.
Artificial Intelligence in DFIR

Al-led digital forensics would allow:

- **Tracing** the evidence in a more enhanced and streamlined fashion to conduct an in-depth investigation
- **Identify** critical forensic evidence and renders it to further analysis objectively and reproducible.
- **Cover** more ground (search and identification) of important trends from large volumes of data followed by visualization of the results
- **Report** investigations results to reveal trends and patterns that were previously unknown
Artificial Intelligence

AI is “the theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages”.

AI would be invaluable in identifying crime as it has been observed that an algorithms based would be more effective in determining the existence of criminal or illegal activity.
Why RL for DFIR – Sequential Decision Process

- RL Agent Mimic Human Expert; **assigned what to do but not how to do it.**
- RL Agent Determine **ideal/best behaviour**; decisions-making sequences to achieve target.

> “Markov Chain: What happens next depends only on the state of affairs now.“

- **Repetitive** tasks with same/different input and parameters
- **No Human expert intervention** during learning process (Reward/punishment feedback).
- RL reflect Action-Effect-Reward characteristic which fully represent DFIR.
- Less time for learning and efficient in sequential decision-making problems if **well represented.**
- RL allow a the **Explainability**

<table>
<thead>
<tr>
<th>Markov Models</th>
<th>Do we have control over the state transitions?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NO</td>
</tr>
<tr>
<td>Are the states completely observable?</td>
<td>YES</td>
</tr>
<tr>
<td>NO</td>
<td>Hidden Markov Model</td>
</tr>
</tbody>
</table>

DFIR as Markov Chain

- E
- 0.3
- 0.7
- 0.4
- 0.6
- A
Reinforcement Learning contribution to DFIR

1. DFIR is rapidly **evolving** and very **complex** environment, therefore representing all these information as MDP is challenging

2. Working with a **Reward Function** to act as feedback provider for the system is a tricky sub-problem (relying on human reward is not practical and **unsafe**)

3. The **Uncertainty** in some of the tasks’ outcome (POMDP is not an option)

4. **Capturing** the Expertise is relative, and the Learning time required for the system to reach **maturity** is uncertain

5. **Scaling-up** and reduce size of MDP environment to allow Solving algorithms performing better.
Explainability: relates to the idea of connecting a machine’s decision-making process with human explanations that are both accurate and understandable.

Interpretability: is the ability to communicate an explanation or meaning in a way that is comprehensible.

Understandability: or intelligibility, refers to the features of a model that allow it to be self-explanatory in terms of its operational functionality without the need to describe its internal structure or the underlying algorithms used to process data.

Transparency: Algorithmic transparency, simulatability, decomposability, and transparency are all characteristics that a transparent model should posses.

Comprehensibility: is often quantified in terms of the model’s complexity, which includes the model’s ability to describe its learning process in a comprehensible manner.
A Markov Decision Process is composed of the following building blocks:

- **State space $S$** — The state contains all possible states whether physical, information or belief attributes, and which the RL agent(s) could face.

- **Action space $A$** — The set containing all (feasible) actions. For state-dependent decisions $a(s)$, it may be necessary to subject the action space to a set of constraints, e.g., using mathematical programming.

- **Reward function $R$** — Denoting the direct reward when taking action $a$ in state $s$.

- **Transition function $T$** — The function governing the dynamics of the system over time, guiding the agent from state $s$ to $s'$. The transition typically involves both a deterministic component (the action $a$) and a stochastic one (exogenous information $\omega$).

- **Discount factor $\gamma$** — Defines the degree to which future rewards impact current decisions. When the problem is infinite-horizon and relies on a cumulative reward objective function, a discount rate $\gamma < 1$ is necessary to ensure convergence.
Research Choices

Evaluation Metrics:

- Consumed time (Criteria 1) - Cost (efficiency)
- Covered Artefacts (Criteria 2)- result reliability (effectiveness)
- Success rate - Subjective

Modelling DFIR

Solving the MDP
RL representation of Incident Response – Malware
Windows Registry (our case study)

registry is a “central hierarchal database” intended to store information that is necessary to configure the system for one or more users, applications, and hardware devices.

- Goldmine for digital forensics.
- Registry Breakdown
- Hives (binary database files)
- Keys & Subkeys (analogous to a folders)
- Values (analogous to a file)
- Type (strings, binary or DWORD)
- Data
Windows Registry Forensics workflow

**Step 1**
Identify File History traces inside target storage devices

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Registry</th>
<th>Event Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existence of configuration files (config.xml)</td>
<td>File History usage status</td>
<td>File History's backup operation logs</td>
</tr>
<tr>
<td>Last backup time</td>
<td></td>
<td>File History related warning/error events</td>
</tr>
</tbody>
</table>

**Step 2**
Determine all devices relating to File History

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Registry</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC information (User name, PC name)</td>
<td>User name, PC name, Drive letter, Volume GUID</td>
</tr>
<tr>
<td>Backup storage information (Volume name, Drive letter, Volume GUID)</td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**
Extract backup file information and analyze actual backup files

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Normalized FileHistory Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup file information in Catalog.edb</td>
<td>Who, PC</td>
</tr>
<tr>
<td>Metadata (name, timestamps) of backed up files stored in backup storage device(s)</td>
<td>Who, User, When, Where, What, Source</td>
</tr>
</tbody>
</table>
Markov Decision Process for Registry Forensics

Diagram:

- **Evidence Reg**
- **HK Local Machine**
- **SAM**
- **SAM-Default-SAM-1000**
- **SAM-SID-500**
- **SAM-Last-Login-DT**

Transition Probabilities and Rewards:

- From **Evidence Reg** to **HK Local Machine**: 0.5, R = 1
- From **HK Local Machine** to **SAM**: 0.5, R = 2
- From **SAM** to **SAM-SID-500**: 0.4, R = 2
- From **SAM-SID-500** to **SAM-Last-Login-DT**: 0.6, R = 2
- From **SAM-Last-Login-DT** to **Evidence Reg**: 0.9, R = 0

Rewards:
- From **Evidence Reg** to **SAM**: R = -1
- From **HK Local Machine** to **Evidence Reg**: R = 1
- From **SAM** to **HK Local Machine**: R = 0
RL representation of Windows Registry Forensics
Results: Solving Time with SD (standard deviation) for different size MDP problems
Results: Number of relevant Artefacts for different size MDP problems
RL contribution to Registry Forensics

- Provides investigators with an “intelligent assistant” that allows cutting in cost (time is money) and avoid delays.

- Makes the practice accessible to non-expert users allowing them to process sensitive forensic information with only minimal technical knowledge.

- Allows learning and expertise capturing and re-use (future similar cases).

- Minimises risks and mistakes (miscarriage of justice) due to human Digital examiners fatigue or misjudgement.
Conclusion and Future works

1. RL works (everyone knows that), it works well in DFIR context despite some challenges.
2. The Proposed Model of Registry Forensics as MDP is fits to purpose (can be extended to further applications)
3. Performance enhancement is clear But we might need to introduction a Hierarchical MDP model
4. Exploration capabilities of the MDP model were beyond expectation and exceed Human expert.
Thank You

Any questions?