LPNMR 2015

13th International Conference on
Logic Programming and Non-monotonic Reasoning

Digital Forensics Evidence Analysis: An Answer Set Programming Approach for Generating Investigation Hypotheses

Stefania Costantini
Giovanni De Gasperis
Raffaele Olivieri

Lexington, KY (USA) September 28, 2015

Who am I ?

Ph.D. Univ. L'Aquila

Off. in Chief of a Unit of RaCIS

Digital Forenser

Agenda:

Research Scope

Digital Forensics

admissibility

The methods must conform to the dictates of the Law

Definition

is a branch of *Criminalistics* which deals with the

- identification
- acquisition
- preservation
- analysis
- presentation

of the information content of (*"Digital Evidence"*) with procedures resistant to any complaints in both civil and criminal court.

Research Scope

Digital Forensics Phases

1. **Identification** → operator → ISO 27037:2012
2. **Acquisition** → dispositivi e tools → Container$_{(DD, EWF, AFF, \ldots)}$
3. **Preservation** → HASH algorithms → Warranty$_{(Integrity\ /\ Authenticity)}$
4. **Analysis** → tool + analyst → Recovery e/o filtering
5. **Presentation** → responsabile → Valutatation and decision

Research Scope

Digital Forensics Phases

1	**Identification**	→	operator	→ ISO 27037:2012
2	**Acquisition**	→	dispositivi e tools	→ Container$_{(DD, EWF, AFF, \ldots)}$
3	**Preservation**	→	HASH algorithms	→ Warranty$_{(Integrity\ /\ Authenticity)}$
4	**Analysis**	→	tool + analyst	→ Recovery e/o filtering
5	**Presentation**	→	responsabile	→ Valutatation and decision

Research Scope

Analysis of *"Digital Evidence"*

Often, different technicians analyzing the same case reach different conclusions, and this may determine different judge's decisions in court.

The analysis of *Digital Evidence* often concerns the examination of incomplete knowledge and or fragmented, and complex scenarios, and includes:

- time evolution
- causation
- uncertainty and doubts
- randomness
- existence of alternative scenarios

Research Scope

Analysis of *"Digital Evidence"*

Often, different technicians analyzing the same case reach different conclusions, and this may determine different judge's decisions in court.

The analysis of *Digital Evidence* often concerns the examination of incomplete knowledge and or fragmented, and complex scenarios, and includes:

- time evolution
- causation
- uncertainty and doubts
- randomness
- existence of alternative scenarios

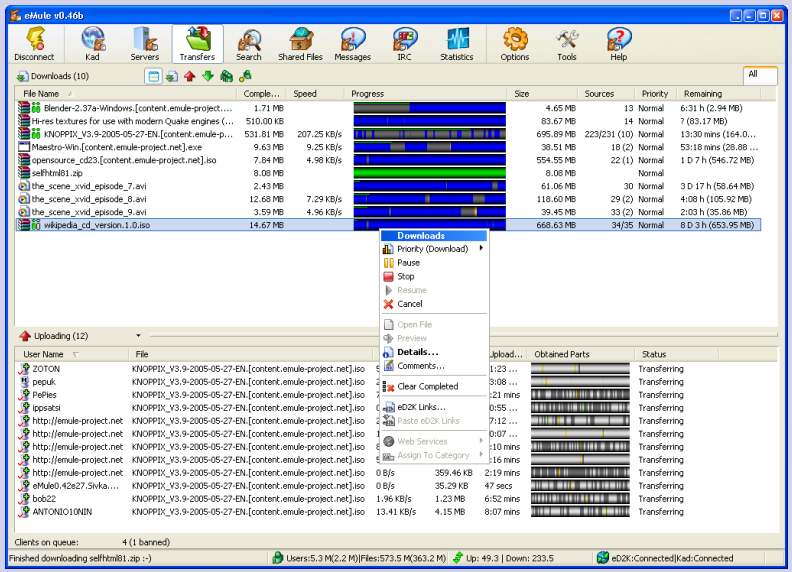
Research Scope

Answer Set Programming

- various investigation cases are reducible to known optimization problems, for which ASP is particularly suitable;
- ease of reading and interpretation
- stable model semantics
- every answer set represents a possible problem solution

Data Recovery & File Sharing Hypotheses

Filesharing



Illicit Files

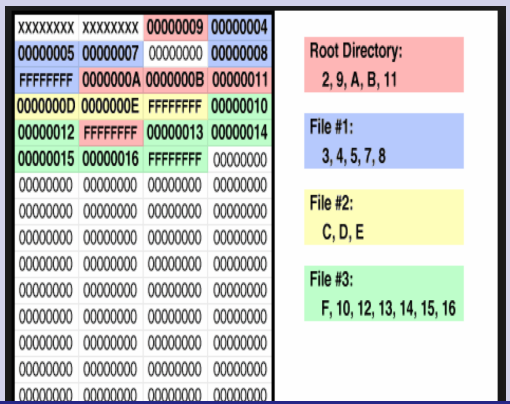
Data Recovery & File Sharing Hypotheses

Memory

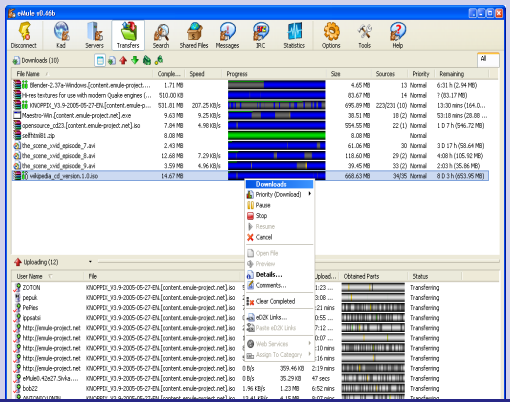
Recovered Files

Illicit Files

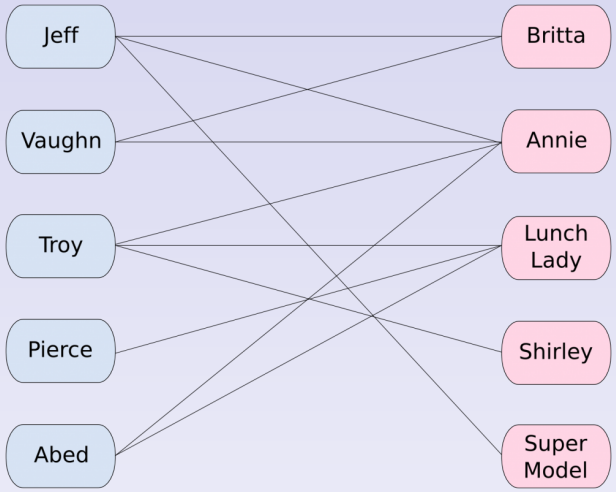
INDX Files



Cache Filesharing



Data Recovery & File Sharing Hypotheses



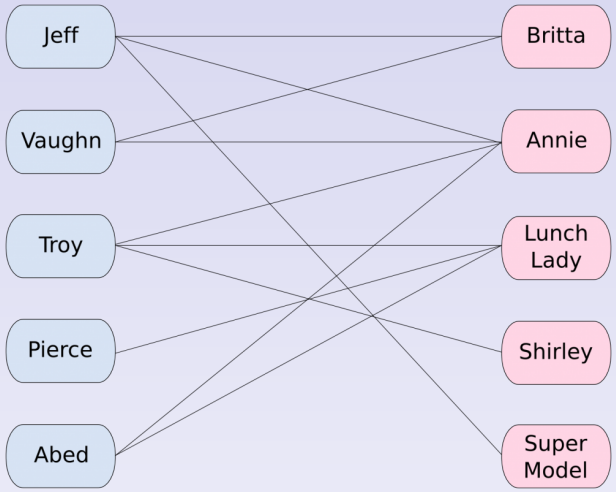
Marriage Problem

knowing the preferences of a group of guys and girls the problem is to pair people so that everyone has a preferred partner to the best possible degree.

Reduction

Men list includes NAMEs of the files contained in INDX files, while Women list consists in the list of name of recovered files. Preferences are elicited from metadata.

Data Recovery & File Sharing Hypotheses



Marriage Problem

knowing the preferences of a group of guys and girls the problem is to pair people so that everyone has a preferred partner to the best possible degree.

Reduction

Men list includes NAMEs of the files contained in INDX files, while Women list consists in the list of name of recovered files. Preferences are elicited from metadata.

Data Recovery & File Sharing Hypotheses

ASP code

```
likes(nome1,file1).
likes(nome1,file2).
likes(nome2,file1).
likes(nome2,file3).
likes(nome2,file2).
likes(nome3,file3).
likes(nome3,file2).
.....
bigamia(X,Y) :- likes(X,Y), likes(X,Y1),
coppia(X,Y), coppia(X,Y1), Y!=Y1.
bigamia(X,Y) :- likes(X,Y), likes(X1,Y),
coppia(X1,Y), X!=X1.
coppia(X,Y) :- likes(X,Y), not bigamia(X,Y).
```

Risultato

```
Answer: 1
Stable Model: coppia(nome3,file2)
coppia(nome2,file3) coppia(nome1,file1)
Answer: 2
Stable Model: coppia(nome3,file3)
coppia(nome2,file1) coppia(nome1,file2)
Answer: 3
Stable Model: coppia(nome3,file3)
coppia(nome2,file2) coppia(nome1,file1)
.....
```

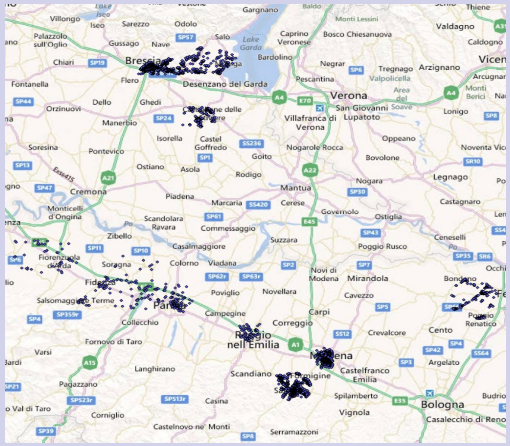
Path Verification

Sexual Abuse

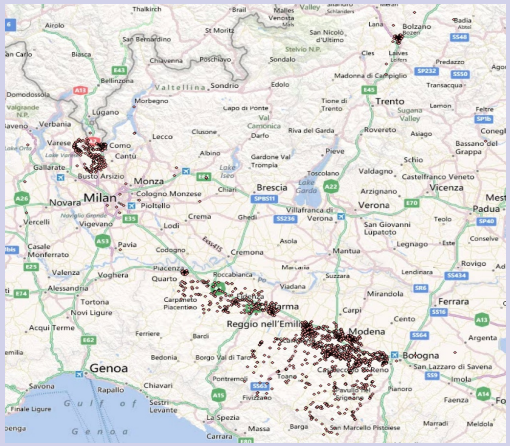
Devices Seized

Path Verification

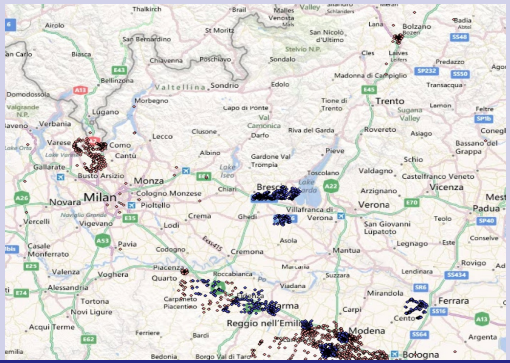
Device 1:



Device 2:



Device 3:



Path Verification

Hidato Matrix

18				26	
19			27		
	14			23	31
1			8	33	
		5			
		10		36	35

Hidato Problem

On a sparse matrix, the goal of Hidato is to fill the array using consecutive numbers in cells adjacent horizontally, vertically or diagonally, creating an ideal path.

Hidato Reduction

The matrix represents the geographic area of interest, where each matrix element represents an area traversable in a unit of time and the value represent the time.

Path Verification

Hidato Matrix

18				26	
19			27		
	14			23	31
1			8	33	
		5			
		10		36	35

Hidato Problem

On a sparse matrix, the goal of Hidato is to fill the array using consecutive numbers in cells adjacent horizontally, vertically or diagonally, creating an ideal path.

Hidato Reduction

The matrix represents the geographic area of interest, where each matrix element represents an area traversable in a unit of time and the value represent the time.

Path Verification

ASP Code

```
#const n = 6.
matrix(1, 1, 18). matrix(1, 5, 26). matrix(2, 1, 19). matrix(2, 4, 27).
matrix(3, 2, 14). matrix(3, 5, 23). matrix(3, 6, 31). matrix(4, 1, 1).
matrix(4, 4, 8). matrix(4, 5, 33). matrix(5, 3, 5). matrix(6, 3, 10).
matrix(6, 5, 36). matrix(6, 6, 35).
size(1..n). values(1..n*n). values2(1..n*n-1). diffs(-1;0;1).

1 x(Row, Col, Value) : values(Value) 1 :- size(Row), size(Col). 1 x(Row, Col,
    Value) : size(Row) : size(Col) 1 :- values(Value). x(Row, Col, Value) :-
    matrix(Row, Col, Value).

valid(Row, Col, Row2, Col2) :- diffs(A), diffs(B), Row2 = Row+A, Col2 = Col+B,
    Row2 >= 1, Col2 >= 1, Row2 <= size, Col2 <= size, size(Row), size(Col).

:- x(Row, Col, Value+1), x(Row2, Col2, Value), not valid(Row, Col, Row2, Col2),
    values2(Value).
```

Path Verification

Results

Answer Set: 1

x(1,1,18) x(1,5,26) x(2,1,19) x(2,4,27) x(3,2,14) x(3,5,23) x(3,6,31)
x(4,1,1) x(4,4,8) x(4,5,33) x(5,3,5) x(6,3,10) x(6,5,36) x(6,6,35) x(5,1,2)
x(6,1,3) x(6,2,4) x(6,4,6) x(5,5,7) x(5,4,9) x(5,2,11) x(4,2,12) x(3,1,13)
x(4,3,15) x(3,3,16) x(2,3,21) x(3,4,22) x(2,6,24) x(1,6,25) x(1,3,28)
x(1,4,29) x(2,5,30) x(4,6,32) x(5,6,34) x(1,2,20) x(2,2,17)

Answer Set: 2

x(1,1,18) x(1,5,26) x(2,1,19) x(2,4,27) x(3,2,14) x(3,5,23) x(3,6,31)
x(4,1,1) x(4,4,8) x(4,5,33) x(5,3,5) x(6,3,10) x(6,5,36) x(6,6,35) x(5,1,2)
x(6,1,3) x(6,2,4) x(6,4,6) x(5,5,7) x(5,4,9) x(5,2,11) x(4,3,12) x(3,3,13)
x(4,2,15) x(3,1,16) x(2,3,21) x(3,4,22) x(2,6,24) x(1,6,25) x(1,3,28)
x(1,4,29) x(2,5,30) x(4,6,32) x(5,6,34) x(1,2,20) x(2,2,17)

Path Verification

Answer Set 1

18	20	28	29	26	25
19	17	21	27	30	24
13	14	16	22	23	31
1	12	15	8	33	32
2	11	5	9	7	34
3	4	10	6	**36**	35

Answer Set 2

18	20	28	29	26	25
19	17	21	27	30	24
16	14	13	22	23	31
1	15	12	8	33	32
2	11	5	9	7	34
3	4	10	6	**36**	35

Alibi Verification

Murder

Suspect Arrested

Alibi Verification

Alibi:

During interrogation the suspect said:

- left his home (place X) at a certain time;
- reached his office (place Y) where he worked on the PC;
- left the Office to go to his friend (place Z) where entering discovered the body;
- called the Police immediatly.

Alibi Verification

To verify the alibi were made the following analysis:

- smartphone's memories of the suspect;
- PC seized in his Office;
- a system of video surveillance installed at a post office, near the place Z, which recorded images of a very crowded street, where the investigators retrive several image sequences where compare a subject with charatteristics compatible with the suspect.

Alibi Verification

Monkey & Banana Problem

The “Monkey & Banana” problem is a typical planning problem.
A monkey is in a room with a chair and a banana tied to the ceiling. The monkey can not reach the banana, unless it is located on the chair. Determine the correct sequence of actions.

Monkey & Banana Reduction

Monkey	→	Suspect
Banana	→	Body
Eats Banana	→	Raise Alarm
Init.ial Position Monkey	→	X
Initial Position Chair	→	Y
Below Banana	→	Z
Walks	→	Walks
Move Chair	→	Motion to Z
Ascend	→	Open the Door
Idle	→	Unknown Action

Alibi Verification

Monkey & Banana Problem

The “Monkey & Banana” problem is a typical planning problem.
A monkey is in a room with a chair and a banana tied to the ceiling. The monkey can not reach the banana, unless it is located on the chair. Determine the correct sequence of actions.

Monkey & Banana Reduction

Monkey	$\rightarrow$	Suspect
Banana	$\rightarrow$	Body
Eats Banana	$\rightarrow$	Raise Alarm
Init.ial Position Monkey	$\rightarrow$	X
Initial Position Chair	$\rightarrow$	Y
Below Banana	$\rightarrow$	Z
Walks	$\rightarrow$	Walks
Move Chair	$\rightarrow$	Motion to Z
Ascend	$\rightarrow$	Open the Door
Idle	$\rightarrow$	Unknown Action

Alibi Verification

Running ASP code we get, among others, the following answer sets that contradict the investigation thesis :

Answer Set 1

step(0, idle, ” ”),
step(1, walk,
chair_starting_point),
step(2, move_chair,
below_banana),
step(3, ascend, ” ”),
step(4, idle, ” ”),
step(5, eats_banana, ” ”)

Answer Set 2

step(0, walk, below_banana),
step(1, walk,
chair_starting_point),
step(2, move_chair,
below_banana),
step(3, ascend, ” ”),
step(4, idle, ” ”),
step(5, eats_banana, ” ”) .

Conclusions

Objectives

- demonstrate the applicability of Logic Programming and non-Monotonic Reasoning to Digital Forensics;
- convince the parties involved in the trial of the limitations of the current analysis techniques;
- provide, in the long term, to police, prosecutors, lawyers, judges, investigators, intelligence agencies, criminologists, etc., with a decision support systems to help them in their activities.

LPNMR 2015

13th International Conference on
Logic Programming and Non-monotonic Reasoning

Digital Forensics Evidence Analysis: An Answer Set Programming Approach for Generating Investigation Hypotheses

Stefania Costantini
Giovanni De Gasperis
Raffaele Olivieri

Lexington, KY (USA) September 28, 2015