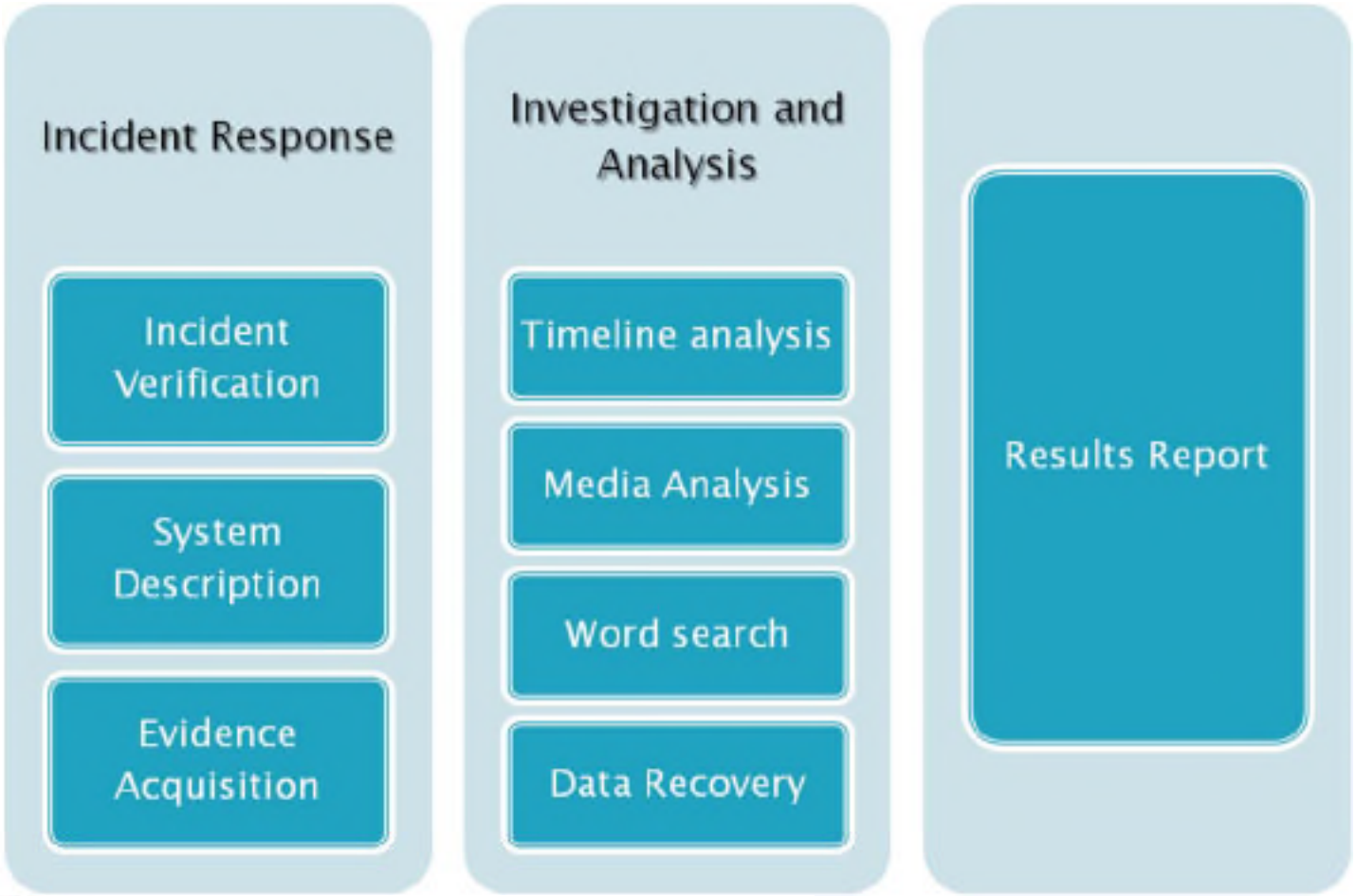
Computer Forensics: From Programming Errors to Antiforensics Techniques: Lessons Learned

Manuel Humberto Santander Peláez
GCFA Gold, GNET Silver, GCIA Gold

Objectives

- Get an insider's view of the forensic investigation process so you can know what to expect
- Identify key tips for forensics investigation
- Discuss common computer forensics patterns
- Examine a practical example: Information theft with Antiforensics techniques
- Examine a practical example: Vulnerability of a program in a banking institution
- Lessons learned

Computer forensics investigation process



Key Tips for Computer Forensics Investigation

- Avoid any modification to the evidence while collecting it or in the analysis process
- Record every piece of evidence you see
- Analyze all collected data from evidence
- Report what you found on an understandable way for everybody

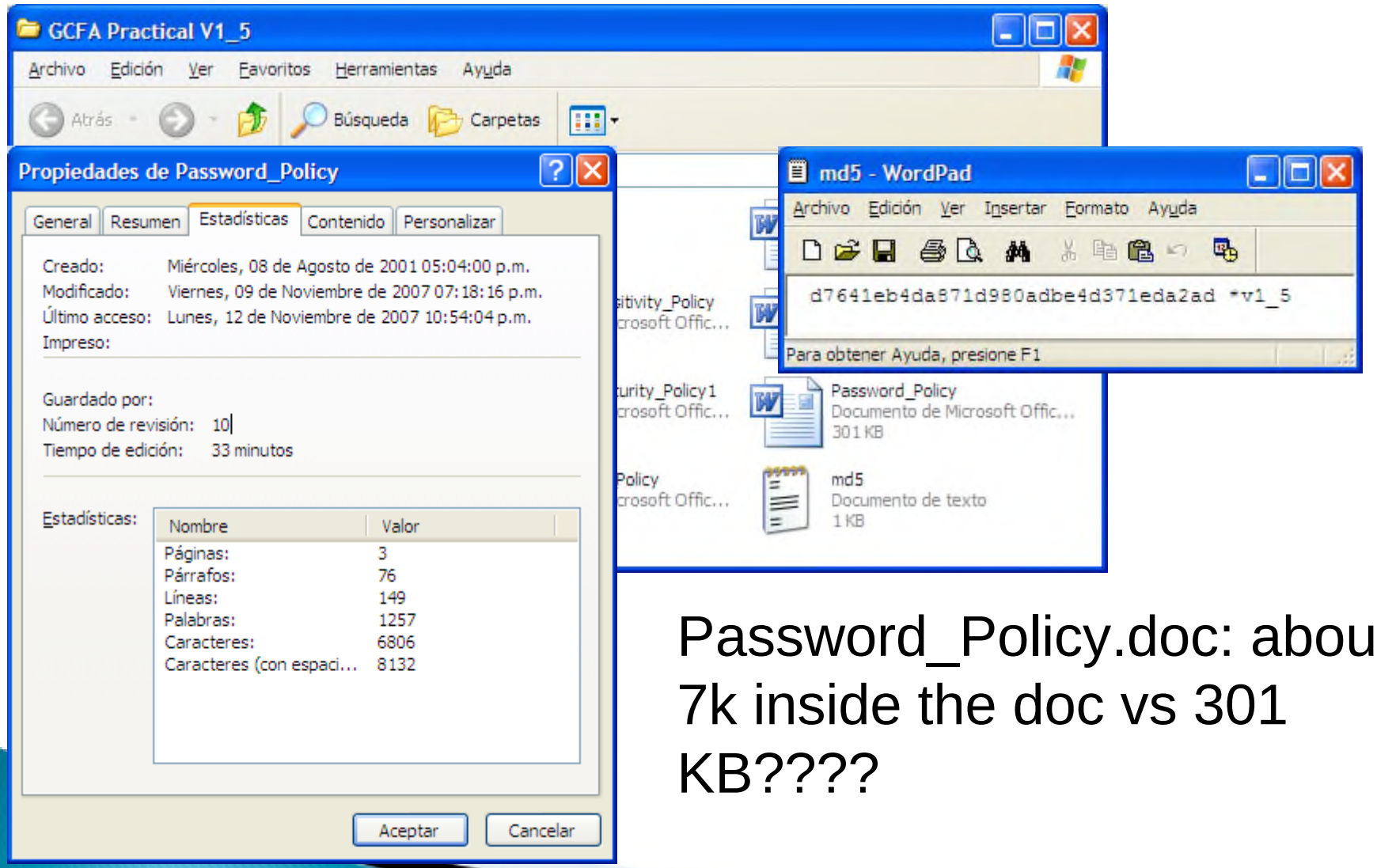
Common computer forensic patterns

- Information robbery
  - By e-mail
  - By removable media devices
  - From a Database
- Electronic money stealing
  - Banking username and password
  - Electronic transfers
  - Update on money or billing databases
- Anonymous mail
  - People threats
  - Sexual harrasment
  - Defamation

Information theft with Antiforensics techniques

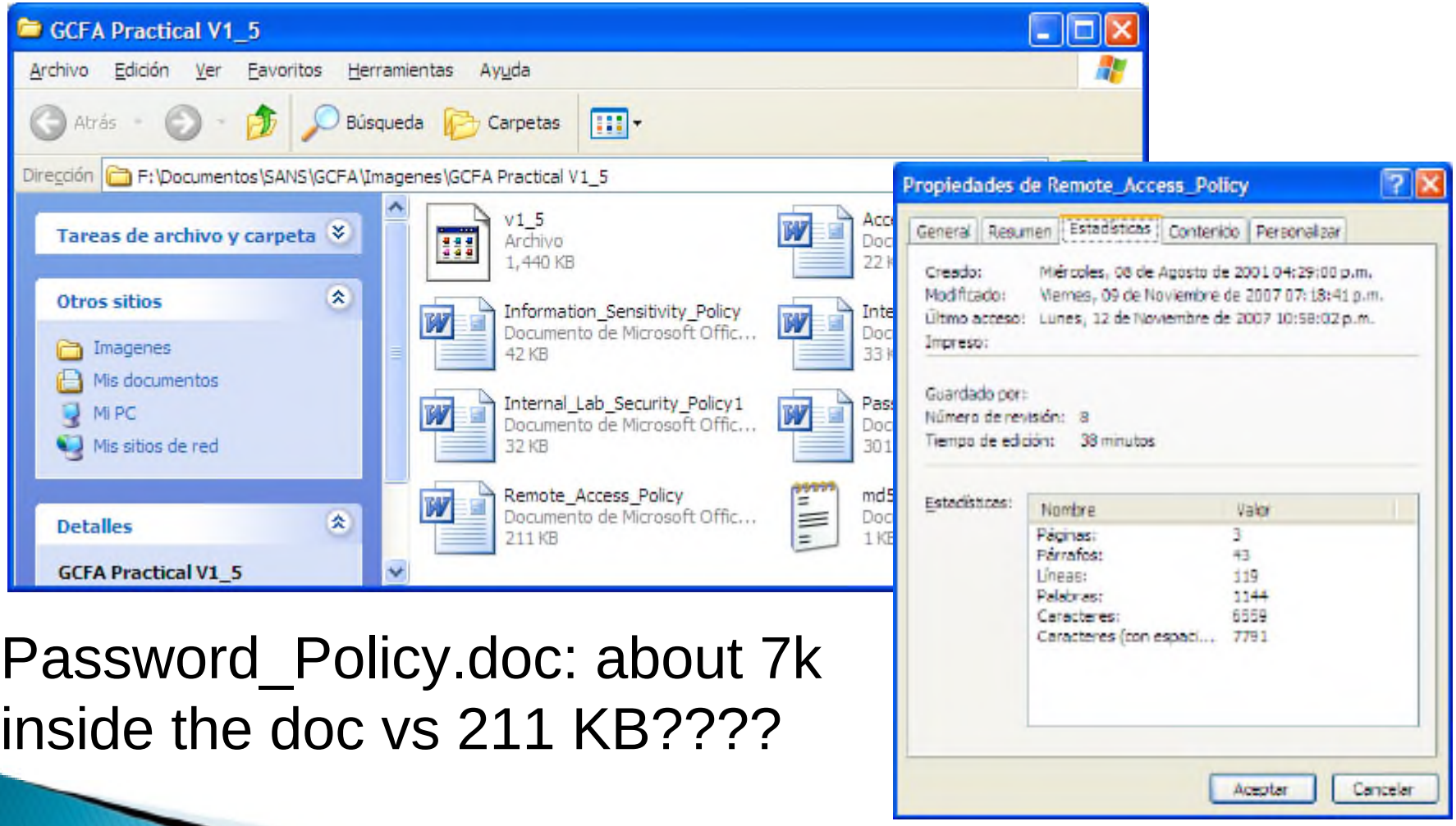
- Ballard industries develops fuel cells
- Secret information that will generate lots of money
- Employee with access to confidential information
- Catched with a floppy on his pocket
- Is he leaking confidential information out of the organization?

Information theft with Antiforensics techniques (2)



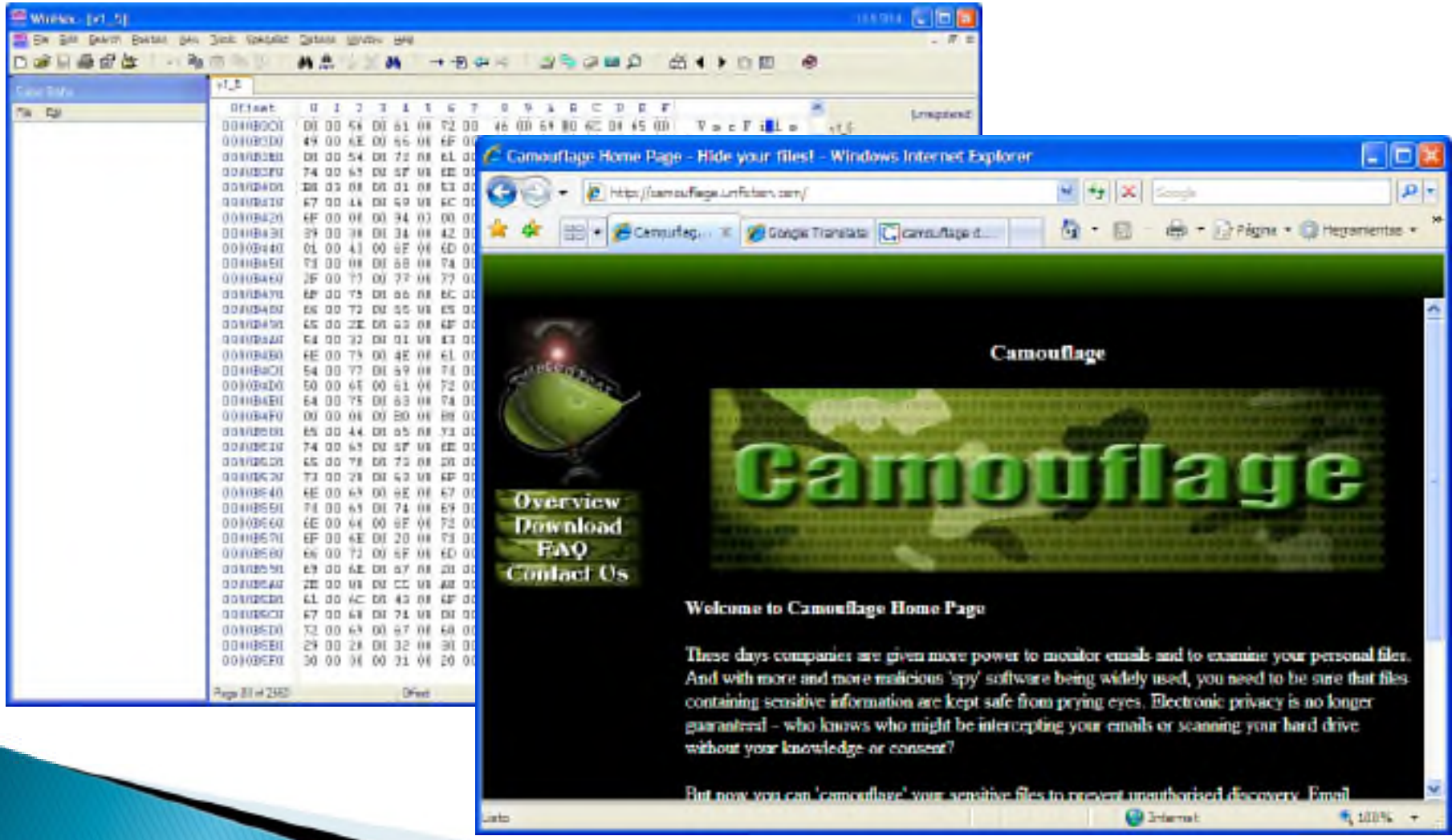
Password_Policy.doc: about 7k inside the doc vs 301 KB????

Information theft with Antiforensics techniques (3)

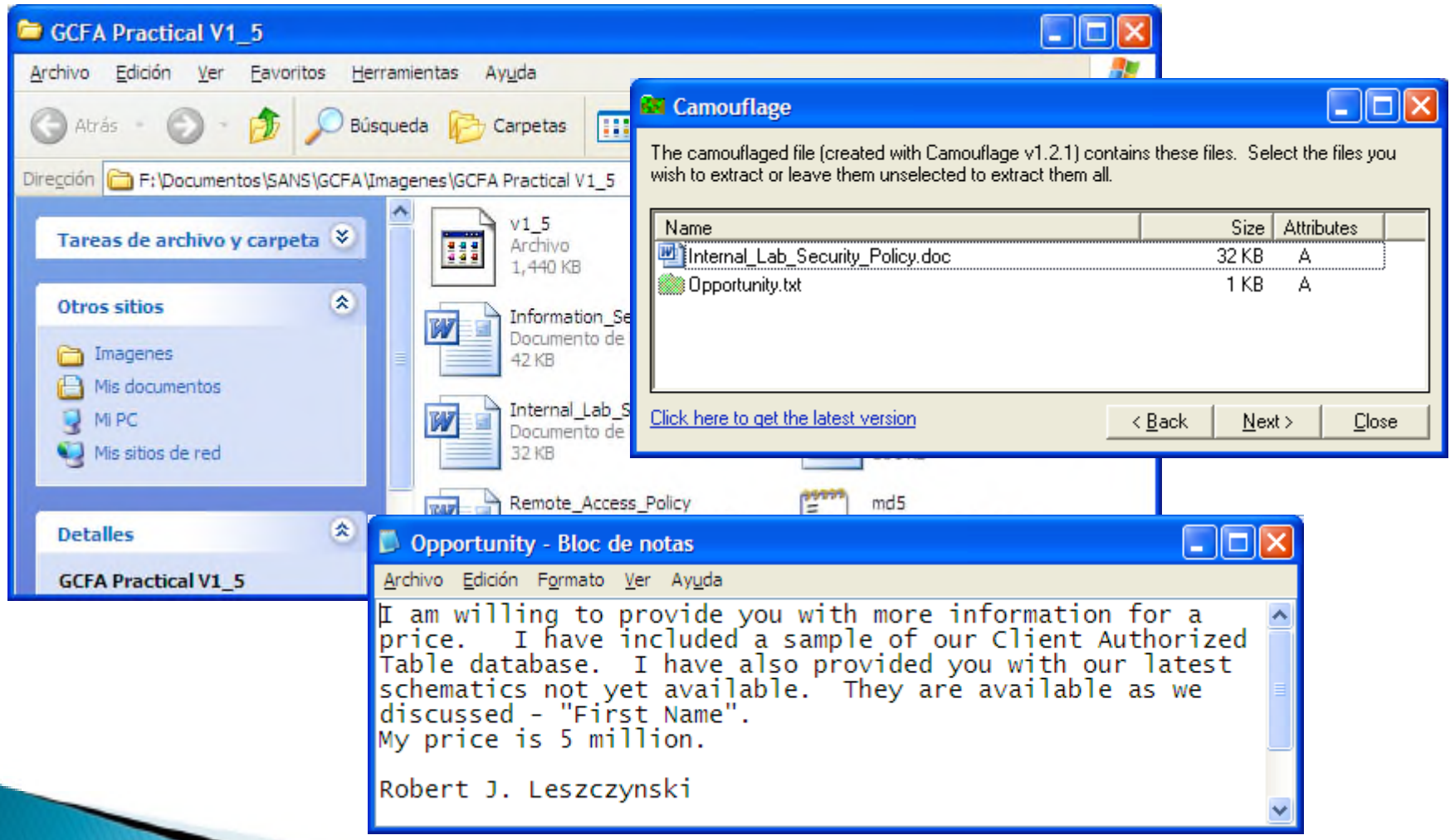


Password_Policy.doc: about 7k inside the doc vs 211 KB????

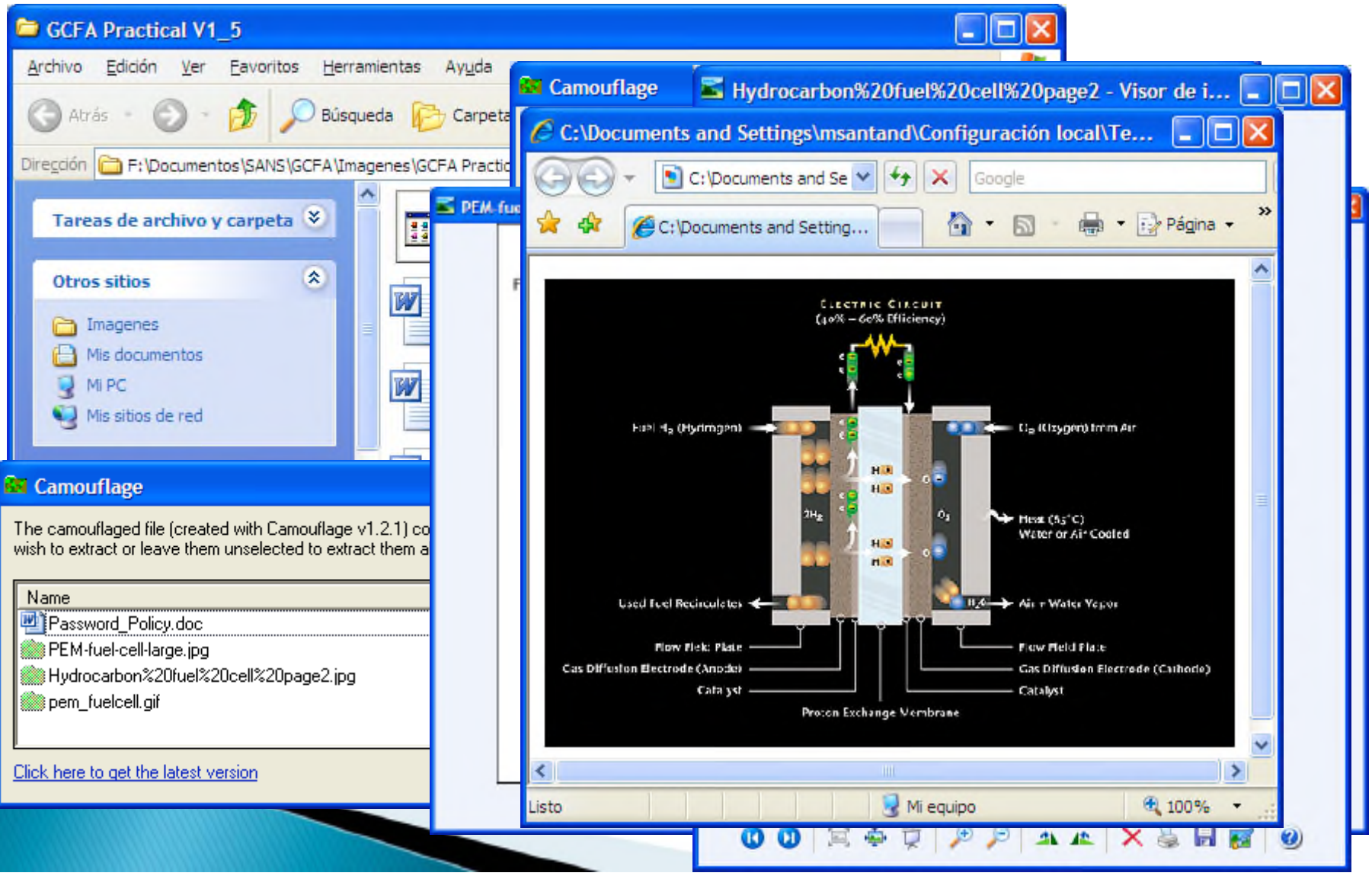
Information theft with Antiforensics techniques (4)



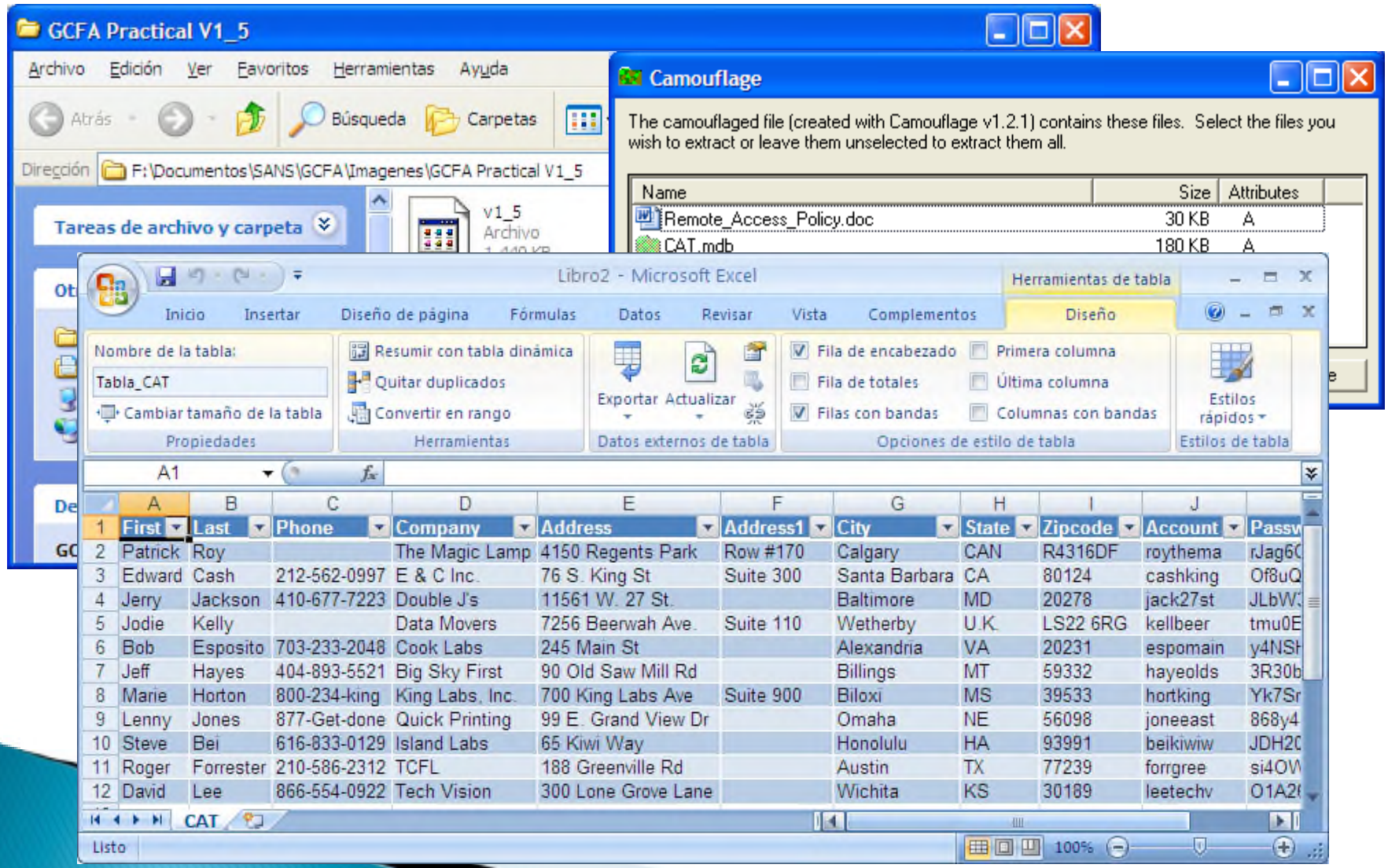
Information theft with Antiforensics techniques (5)



Information theft with Antiforensics techniques (6)



Information theft with Antiforensics techniques (7)



	A	B	C	D	E	F	G	H	I	J	
1	First	Last	Phone	Company	Address	Address1	City	State	Zipcode	Account	Passw
2	Patrick	Roy		The Magic Lamp	4150 Regents Park	Row #170	Calgary	CAN	R4316DF	roythema	rJag6(
3	Edward	Cash	212-562-0997	E & C Inc.	76 S. King St	Suite 300	Santa Barbara	CA	80124	cashking	Of8uQ
4	Jerry	Jackson	410-677-7223	Double J's	11561 W. 27 St.		Baltimore	MD	20278	jack27st	JLbW
5	Jodie	Kelly		Data Movers	7256 Beerwah Ave.	Suite 110	Wetherby	U.K.	LS22 6RG	kellbeer	tmu0E
6	Bob	Esposito	703-233-2048	Cook Labs	245 Main St		Alexandria	VA	20231	espomain	y4NSh
7	Jeff	Hayes	404-893-5521	Big Sky First	90 Old Saw Mill Rd		Billings	MT	59332	hayeolds	3R30b
8	Marie	Horton	800-234-king	King Labs, Inc.	700 King Labs Ave	Suite 900	Biloxi	MS	39533	hortking	Yk7Sr
9	Lenny	Jones	877-Get-done	Quick Printing	99 E. Grand View Dr		Omaha	NE	56098	joneeast	868y4
10	Steve	Bei	616-833-0129	Island Labs	65 Kiwi Way		Honolulu	HA	93991	beikiwiw	JDH2(
11	Roger	Forrester	210-586-2312	TCFL	188 Greenville Rd		Austin	TX	77239	forrgree	si4OW
12	David	Lee	866-554-0922	Tech Vision	300 Lone Grove Lane		Wichita	KS	30189	leetechv	O1A2(

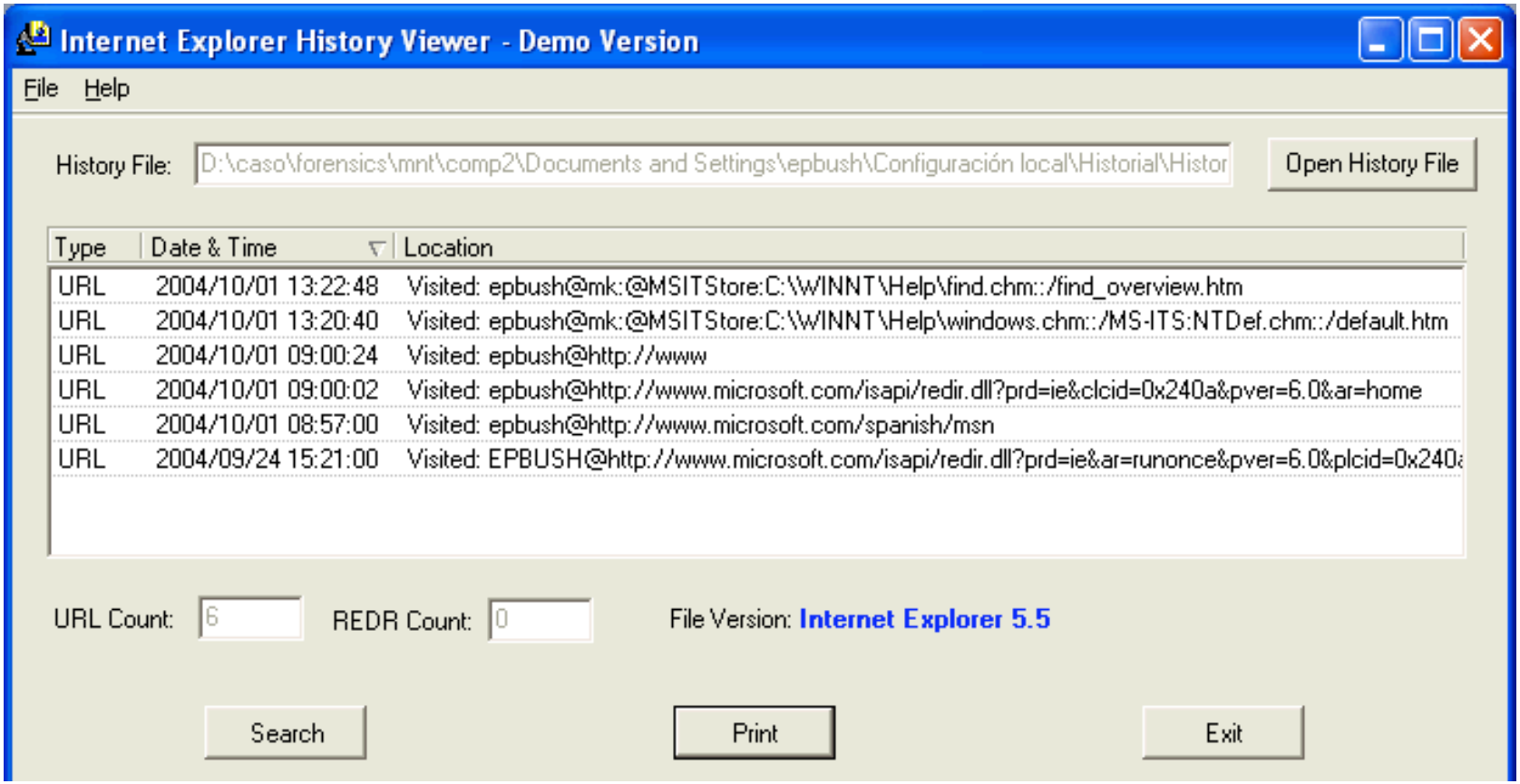
Vulnerability of a critical program in a banking institution

- Bank has points of service where people can do deposits, withdrawals, bill payments and transfers
- The cashier has a POS terminal where people sweeps their debit card, types the PIN and then performs the requested operations
- One of the offices at Barranquilla reported a massive card cloning with the corresponding money stealing
- Only transactions from one cashier are suspicious

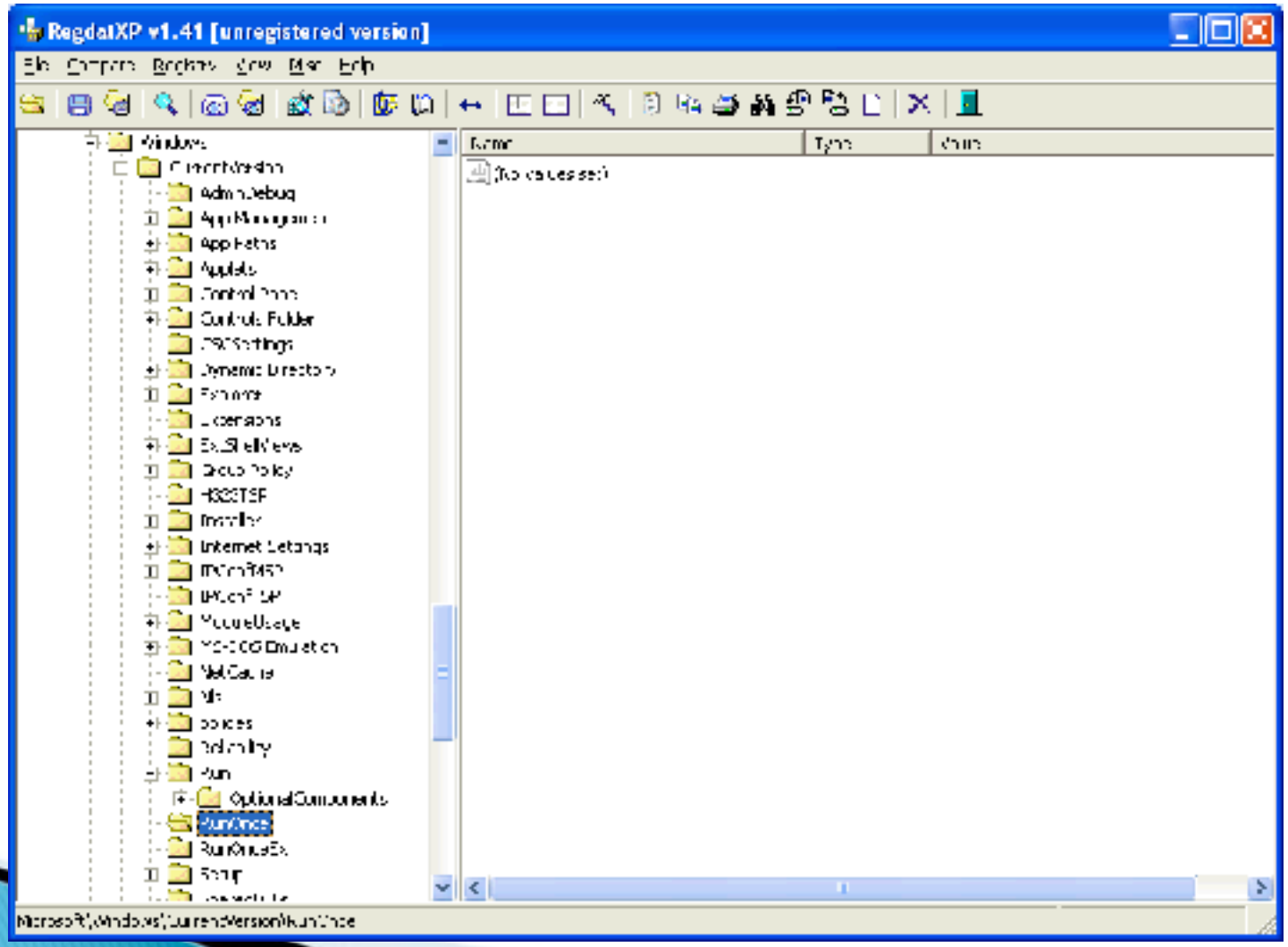
Vulnerability of a critical program in a banking institution (2)

- Information Leak can be done:
  - Using Internet Explorer
  - From the Network
  - Trojan programs used as a backdoor for a specific computer
  - Malicious services installed on the machine
- Timeline doesn't show any abnormal activity like a massive copy, trojan installation or security breach
- The computer was checked for all the possible symptoms and none were found

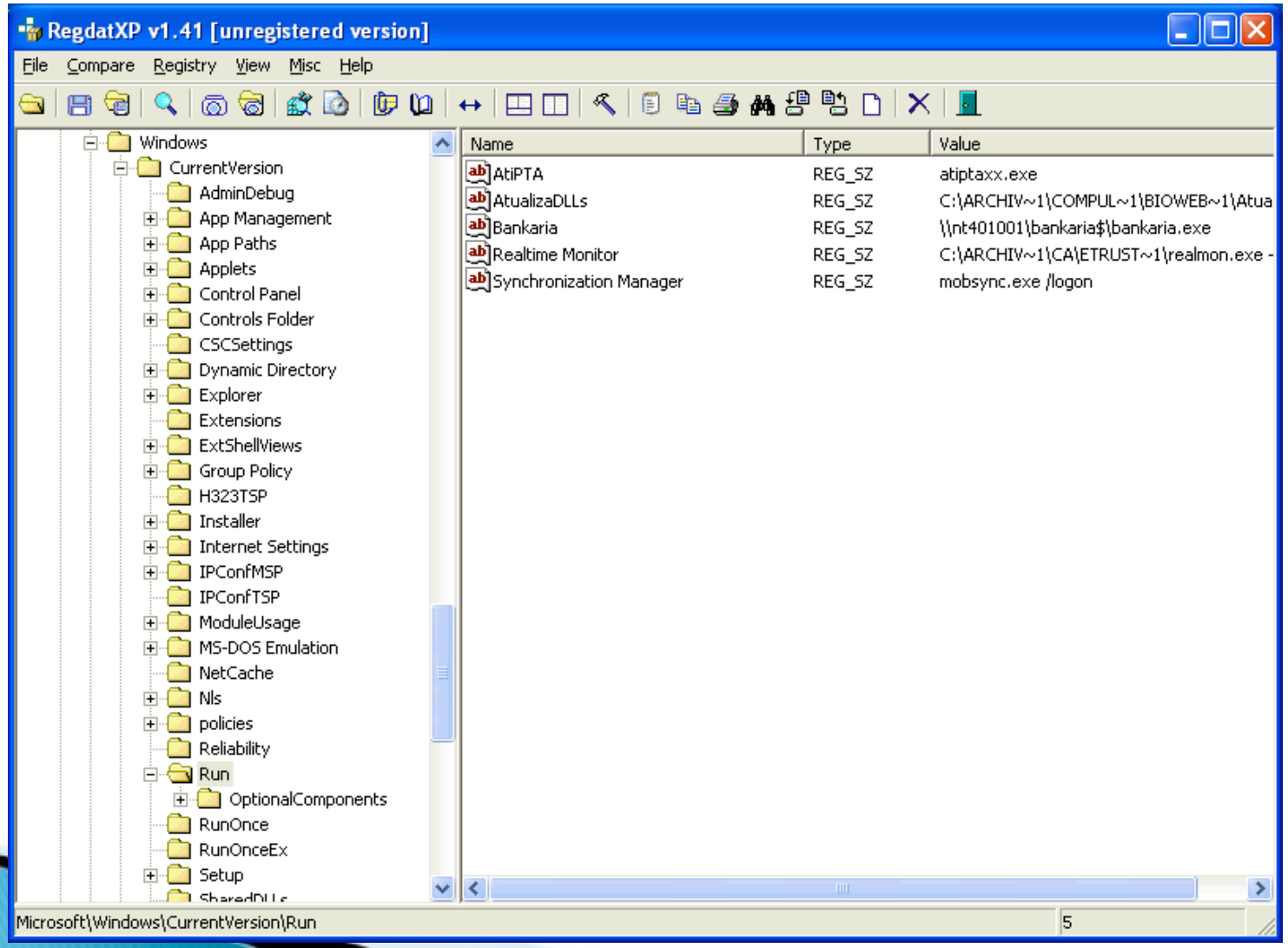
Vulnerability of a critical program in a banking institution (3)



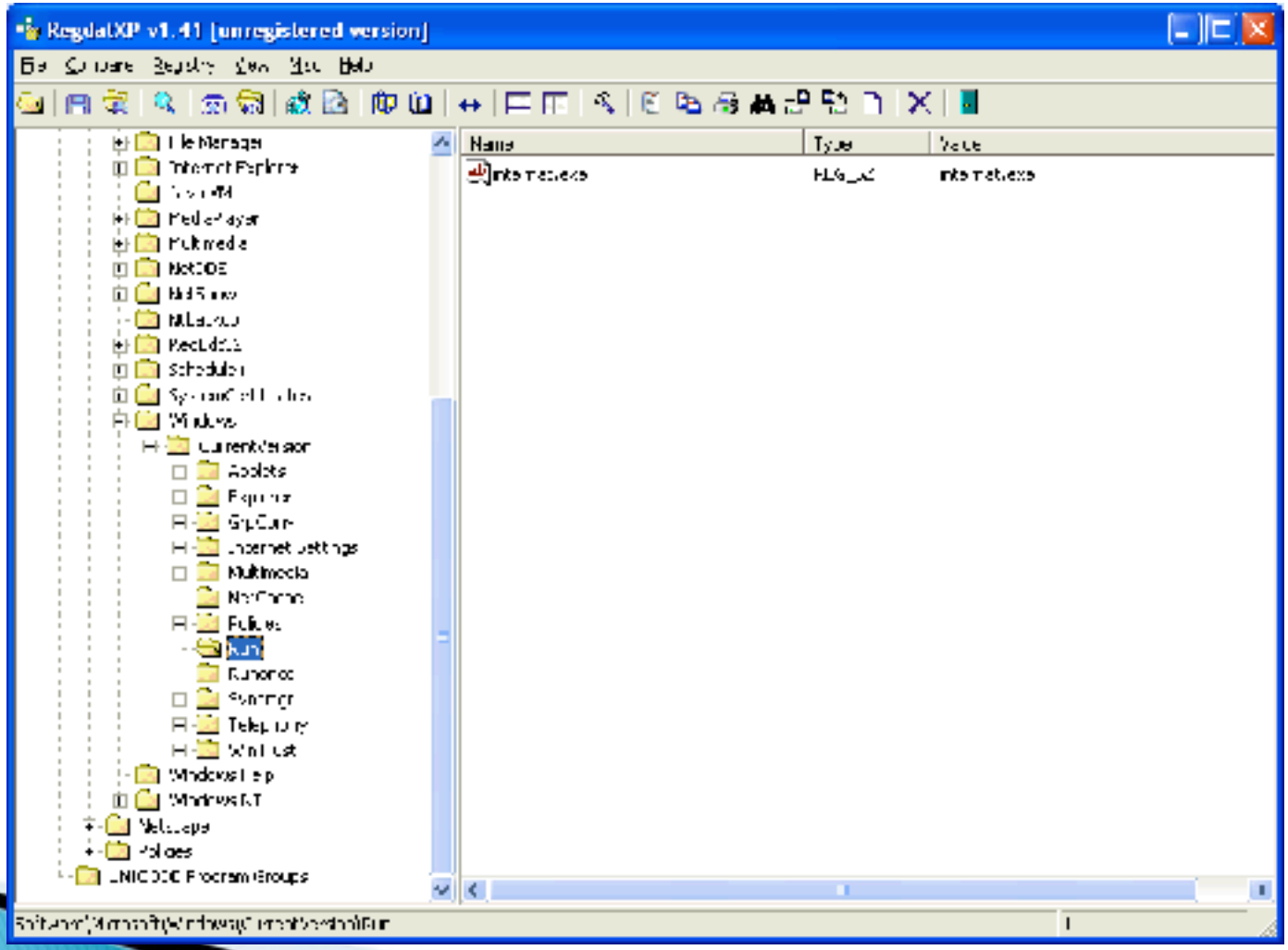
Vulnerability of a critical program in a banking institution (4)



Vulnerability of a critical program in a banking institution (5)



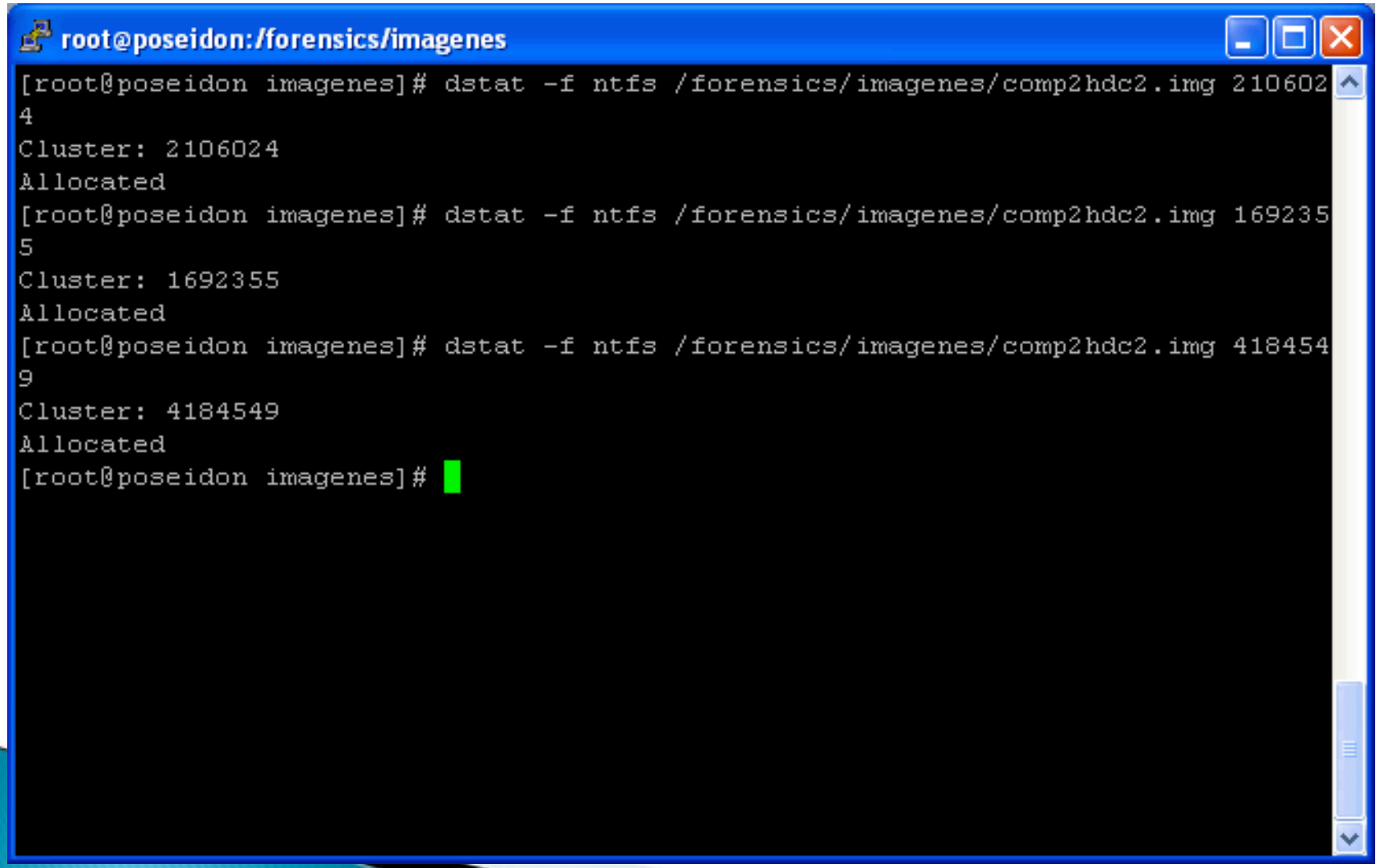
Vulnerability of a critical program in a banking institution (6)



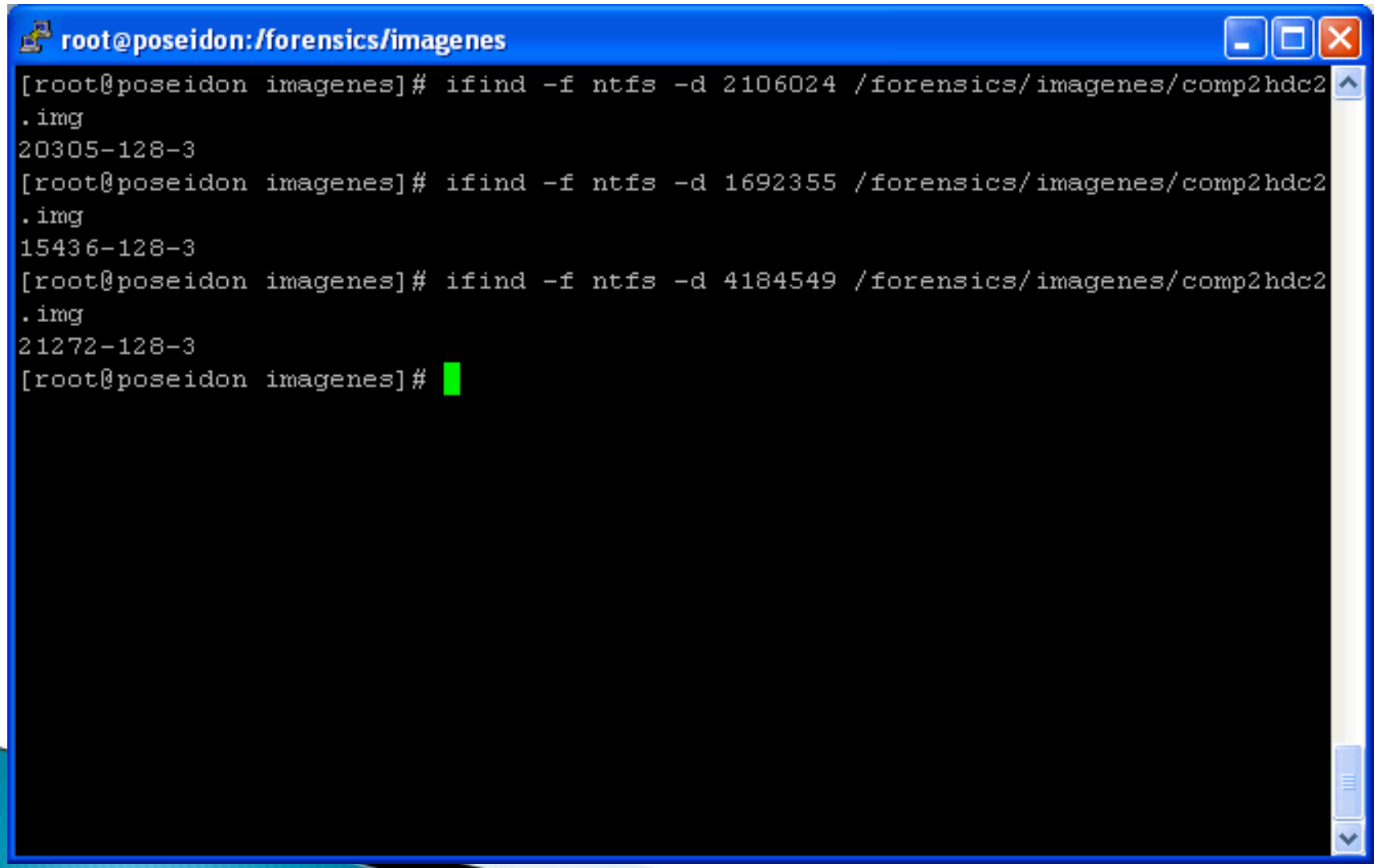
Vulnerability of a critical program in a banking institution (7)

- Detailed file search must be performed
  - Only way to clone a card is to copy the magnetic stripe
  - If the users didn't lent the card, magnetic stripes must be somewhere
  - Strings files from images are generated and then the starter string of every magnetic stripe for the bank is searched
- Many strings matches the search on the image
- Terminal program records every magnetic stripe from every card passed on the reader

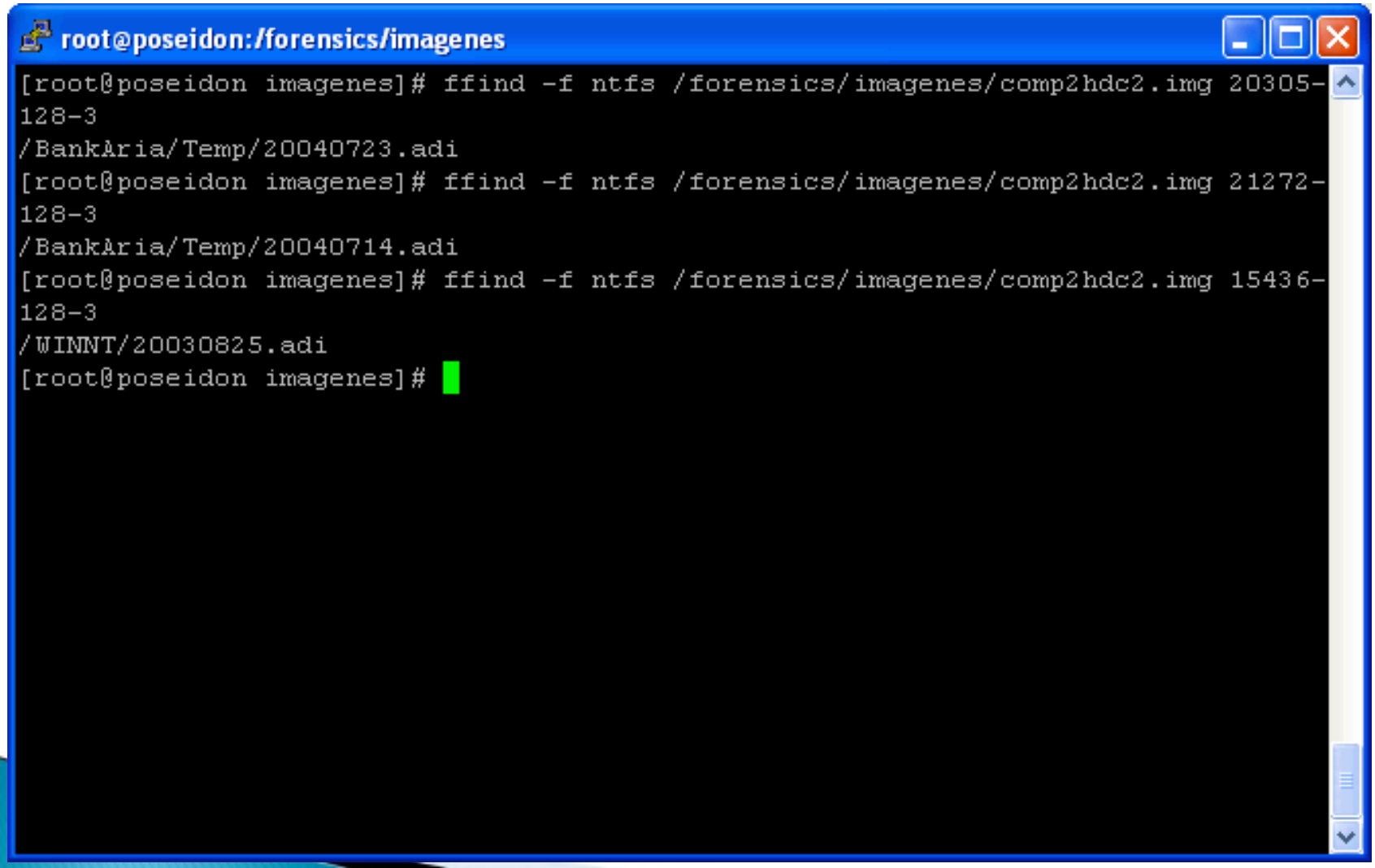
Vulnerability of a critical program in a banking institution (8)



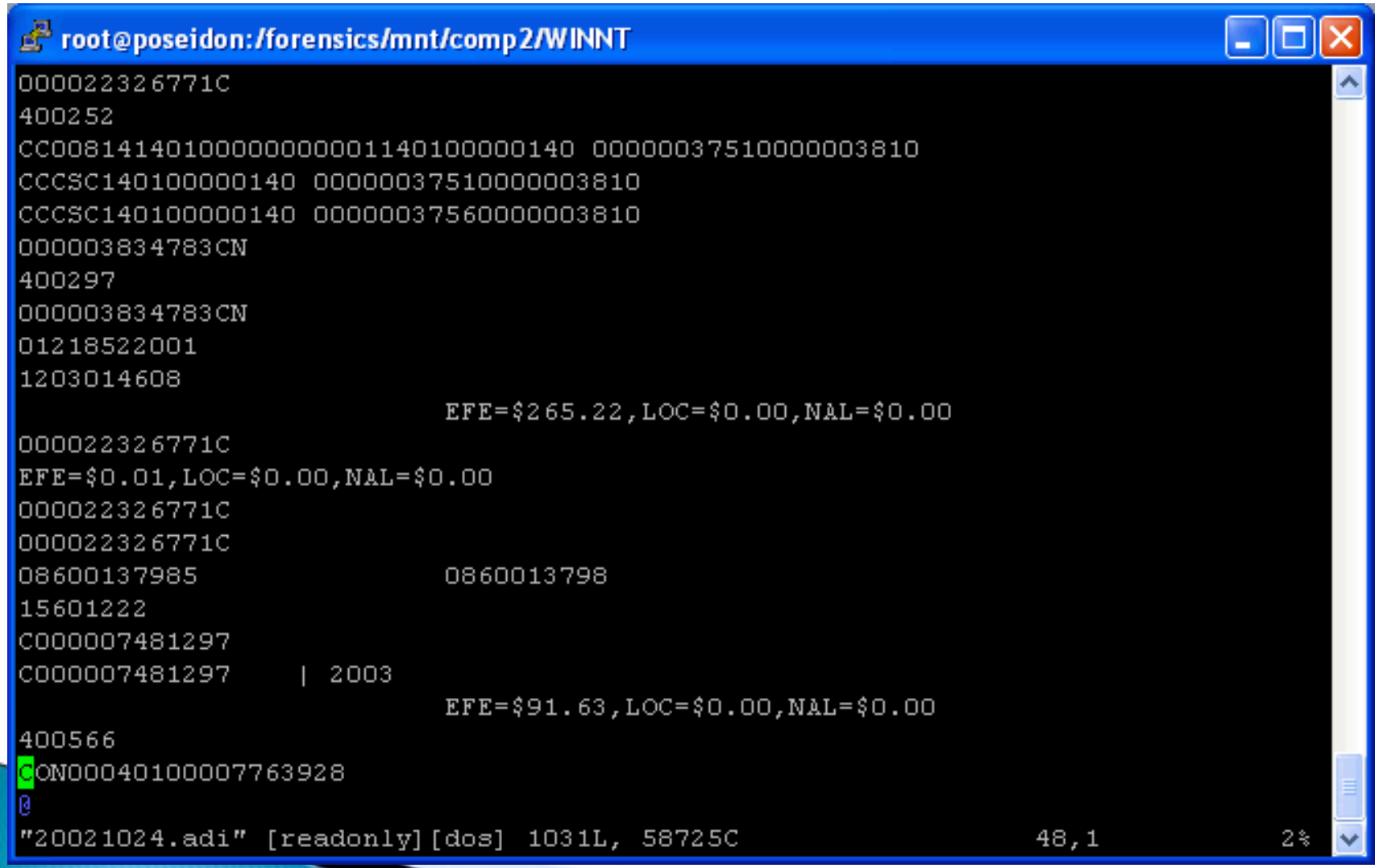
Vulnerability of a critical program in a banking institution (9)



Vulnerability of a critical program in a banking institution (10)



Vulnerability of a critical program in a banking institution (11)



Lessons learned

- Computer Security Incidents REALLY happens
- What seems to be might not be at all
- Computer Security Architecture REALLY helps on a computer forensics investigation by providing valid evidence to correlate within the local storage media of the suspicious computer
- Even if you have a very good security architecture, program bugs might override all registers configured and make possible a computer fraud without valid proof.