

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

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

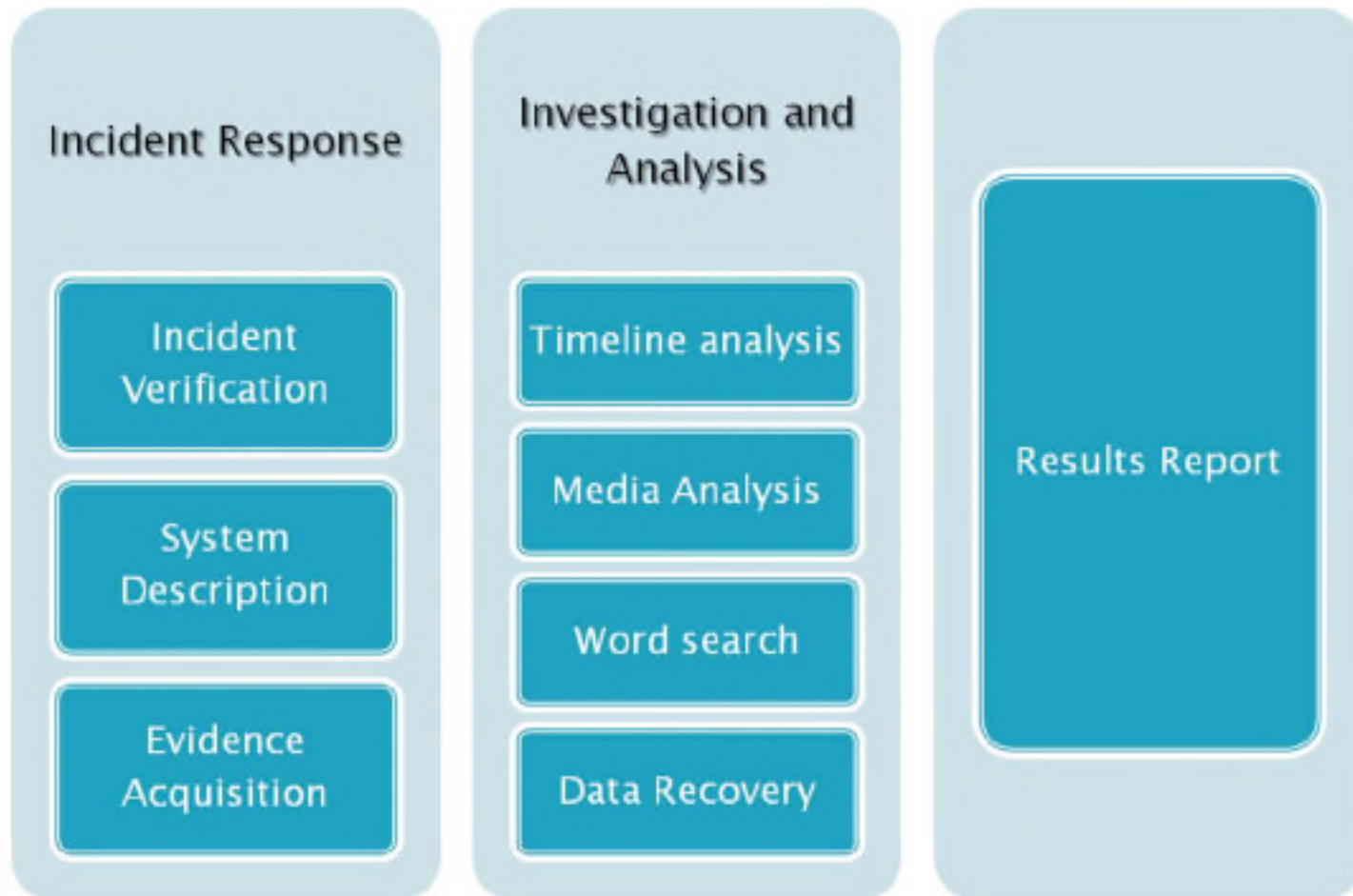


Objectives

- ▶ 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
- ▶ Caught with a floppy on his pocket
- ▶ Is he leaking confidential information out of the organization?



Information theft with Antiforensics techniques (2)

The screenshot shows a Windows XP desktop environment. In the background, a file explorer window titled 'GCFA Practical V1_5' is open. In the foreground, a 'Propiedades de Password_Policy' dialog box is open, showing the 'Estadísticas' tab. The statistics for 'Password_Policy.doc' are as follows:

Nombre	Valor
Páginas:	3
Párrafos:	76
Líneas:	149
Palabras:	1257
Caracteres:	6806
Caracteres (con espaci...)	8132

Below the statistics table are 'Aceptar' and 'Cancelar' buttons. To the right, a 'md5 - WordPad' window is open, displaying the MD5 hash: 'd7641eb4da871d980adbe4d371eda2ad *v1_5'. The WordPad window also shows a menu bar and a toolbar.

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

Information theft with Antiforensics techniques (3)

GCFA Practical V1_5

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Carpetas

Dirección F:\Documentos\SANS\GCFA\Imágenes\GCFA Practical V1_5

Tareas de archivo y carpeta

Otros sitios

- Imágenes
- Mis documentos
- Mi PC
- Mis sitios de red

Detalles

GCFA Practical V1_5

v1_5 Archivo 1,440 KB

Information_Sensitivity_Policy Documento de Microsoft Office... 42 KB

Internal_Lab_Security_Policy1 Documento de Microsoft Office... 32 KB

Remote_Access_Policy Documento de Microsoft Office... 211 KB

Propiedades de Remote_Access_Policy

General Resumen Estadísticas Contenido Personalizar

Creado: Miércoles, 08 de Agosto de 2007 04:29:00 p.m.
Modificado: Viernes, 09 de Noviembre de 2007 07:18:41 p.m.
Último acceso: Lunes, 12 de Noviembre de 2007 10:58:02 p.m.
Impreso:

Guardado por:
Número de revisión: 8
Tiempo de edición: 38 minutos

Estadísticas:

Nombre	Valor
Páginas:	3
Párrafos:	43
Líneas:	119
Palabras:	1144
Caracteres:	6559
Caracteres (con espaci...:	7791

Aceptar Cancelar

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

Information theft with Antiforensics techniques (4)

The image shows a Windows XP desktop environment. On the left, a hex editor window titled 'WinHex [v1.5]' is open, displaying a hex dump of data. The hex dump shows a sequence of bytes, with some characters visible in the ASCII column on the right, including 'Camouflage'. The main window is a Windows Internet Explorer browser displaying the 'Camouflage Home Page'. The browser's address bar shows the URL 'https://camouflage.unfiction.com/'. The page features a green and black camouflage theme. A navigation menu on the left includes links for 'Overview', 'Download', 'FAQ', and 'Contact Us'. The main content area has the word 'Camouflage' in large green letters. Below this, there is a 'Welcome to Camouflage Home Page' section with a paragraph of text: 'These days companies are given more power to monitor emails and to examine your personal files. And with more and more malicious 'spy' software being widely used, you need to be sure that files containing sensitive information are kept safe from prying eyes. Electronic privacy is no longer guaranteed - who knows who might be intercepting your emails or scanning your hard drive without your knowledge or consent? But now you can 'camouflage' your sensitive files to prevent unauthorised discovery. Email

Information theft with Antiforensics techniques (5)

The screenshot displays a Windows XP desktop environment. In the background, a File Explorer window titled "GCFA Practical V1_5" is open, showing a folder structure with files like "v1_5", "Information_Se", "Internal_Lab_S", and "Remote_Access_Policy".

In the foreground, a "Camouflage" dialog box is open. It contains the following text: "The camouflaged file (created with Camouflage v1.2.1) contains these files. Select the files you wish to extract or leave them unselected to extract them all." Below this text is a table with three columns: "Name", "Size", and "Attributes".

Name	Size	Attributes
Internal_Lab_Security_Policy.doc	32 KB	A
Opportunity.txt	1 KB	A

At the bottom of the dialog box, there is a link: "Click here to get the latest version" and three buttons: "< Back", "Next >", and "Close".

Below the dialog box, a Notepad window titled "Opportunity - Bloc de notas" is open. It contains the following text:

I am willing to provide you with more information for a price. I have included a sample of our Client Authorized Table database. I have also provided you with our latest schematics not yet available. They are available as we discussed - "First Name". My price is 5 million.

Robert J. Leszczynski

Information theft with Antiforensics techniques (6)

The screenshot illustrates a Windows XP desktop environment used for information theft. It features three overlapping windows:

- File Explorer (GCFA Practical V1_5):** Shows a folder structure with 'Tareas de archivo y carpeta' and 'Otros sitios'. A file named 'pem_fuelcell.gif' is highlighted in the list.
- Camouflage Utility:** A window titled 'Camouflage' with the text: 'The camouflaged file (created with Camouflage v1.2.1) can wish to extract or leave them unselected to extract them a'. Below this is a list of files: 'Password_Policy.doc', 'PEM-fuel-cell-large.jpg', 'Hydrocarbon%20fuel%20cell%20page2.jpg', and 'pem_fuelcell.gif'. A link at the bottom says 'Click here to get the latest version'.
- Internet Explorer (Hydrocarbon%20fuel%20cell%20page2 - Visor de i...):** Displays a diagram of a Proton Exchange Membrane (PEM) fuel cell. The diagram is titled 'ELECTRIC CIRCUIT (10% - 60% Efficiency)'. It shows the flow of H_2 (Hydrogen) and O_2 (Oxygen from Air) into the cell, the flow of electrons (e^-) through an external circuit, and the flow of protons (H^+) through the membrane. Labels include: 'Used Fuel Recirculates', 'Flow Field Plate', 'Gas Diffusion Electrode (Anode)', 'Catalyst', 'Proton Exchange Membrane', 'Flow Field Plate', 'Gas Diffusion Electrode (Cathode)', 'Catalyst', and 'Flow (55°C) Water or Air Cooled'. The output is labeled 'Air + Water Vapor'.

Information theft with Antiforensics techniques (7)

The screenshot shows a Windows desktop environment with three overlapping windows:

- Windows Explorer:** Displays the folder 'GCFA Practical V1_5' at the path 'F:\Documentos\SANS\GCFA\Imágenes\GCFA Practical V1_5'. It shows a file named 'v1_5' (Archivo, 1.140 KB).
- Camouflage:** A dialog box titled 'Camouflage' with the text: 'The camouflaged file (created with Camouflage v1.2.1) contains these files. Select the files you wish to extract or leave them unselected to extract them all.' It contains a table with the following data:

Name	Size	Attributes
Remote_Access_Policy.doc	30 KB	A
CAT.mdb	180 KB	A
- Microsoft Excel:** A spreadsheet titled 'Libro2 - Microsoft Excel' with a table named 'Tabla_CAT'. The table has the following columns and data:

	A	B	C	D	E	F	G	H	I	J	K
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	rJag6C
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	y4NSt
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	JDH2C
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

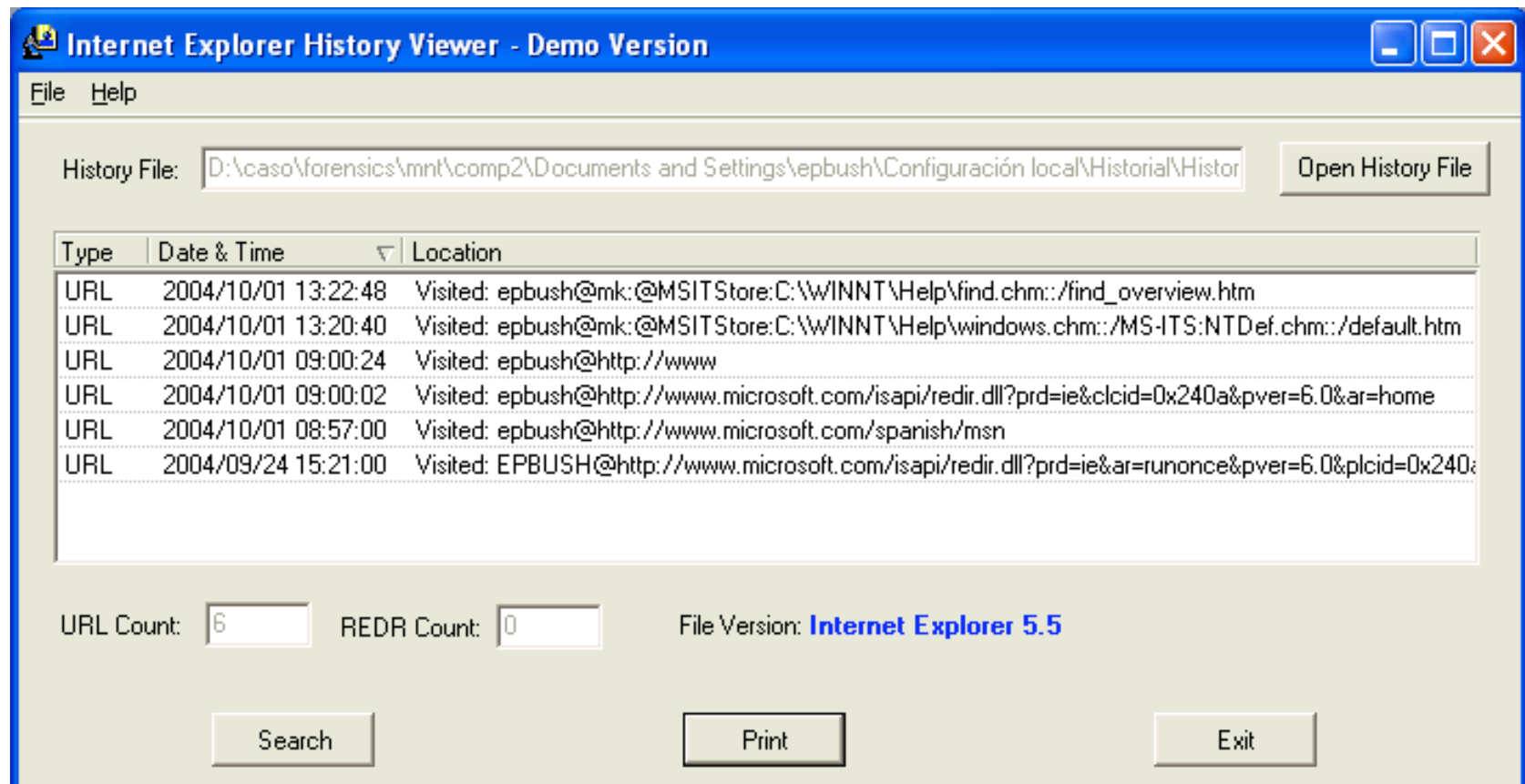


Vulnerability of a critical program in a banking institution (2)

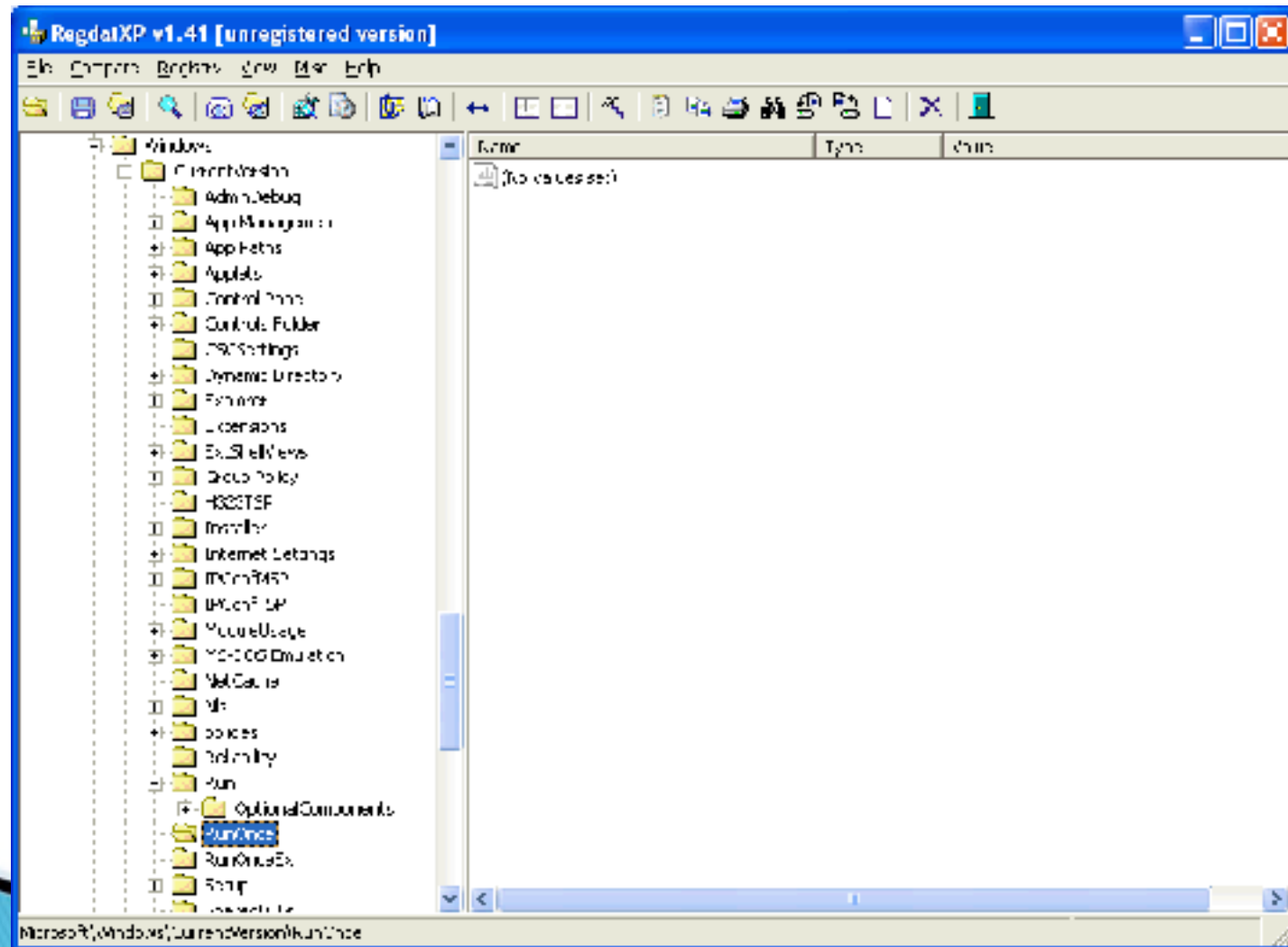
- ▶ Information Leak can be done:
 - ❖ Using Internet Explorer
 - ❖ From the Network
 - ❖ Trojan programs used as a backdoor for a specific computer
 - ❖ Malicious services installed on the machine
- ▶ Timeline doesn't show any abnormal activity like a massive copy, trojan installation or security breach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



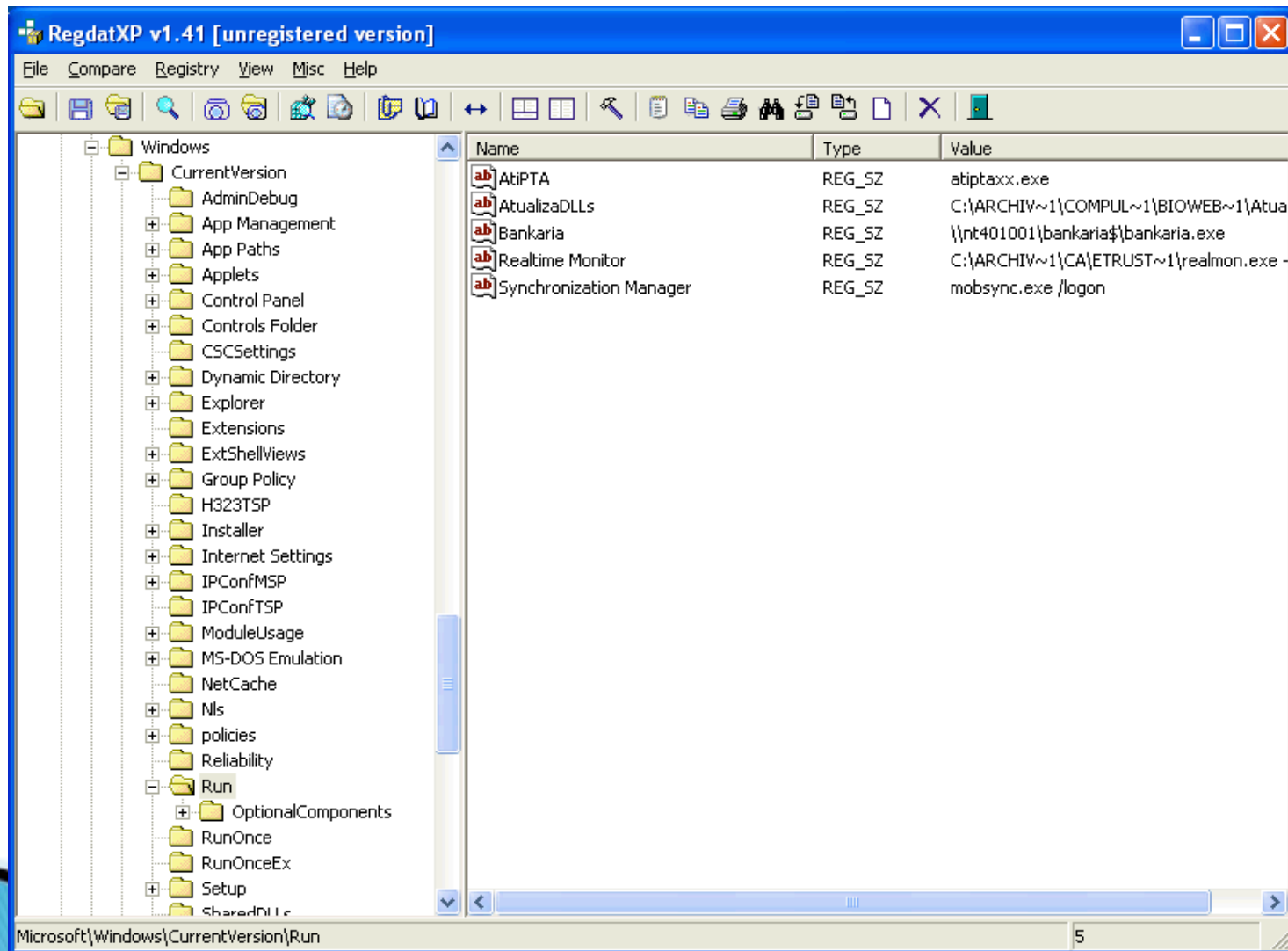
Vulnerability of a critical program in a banking institution (3)



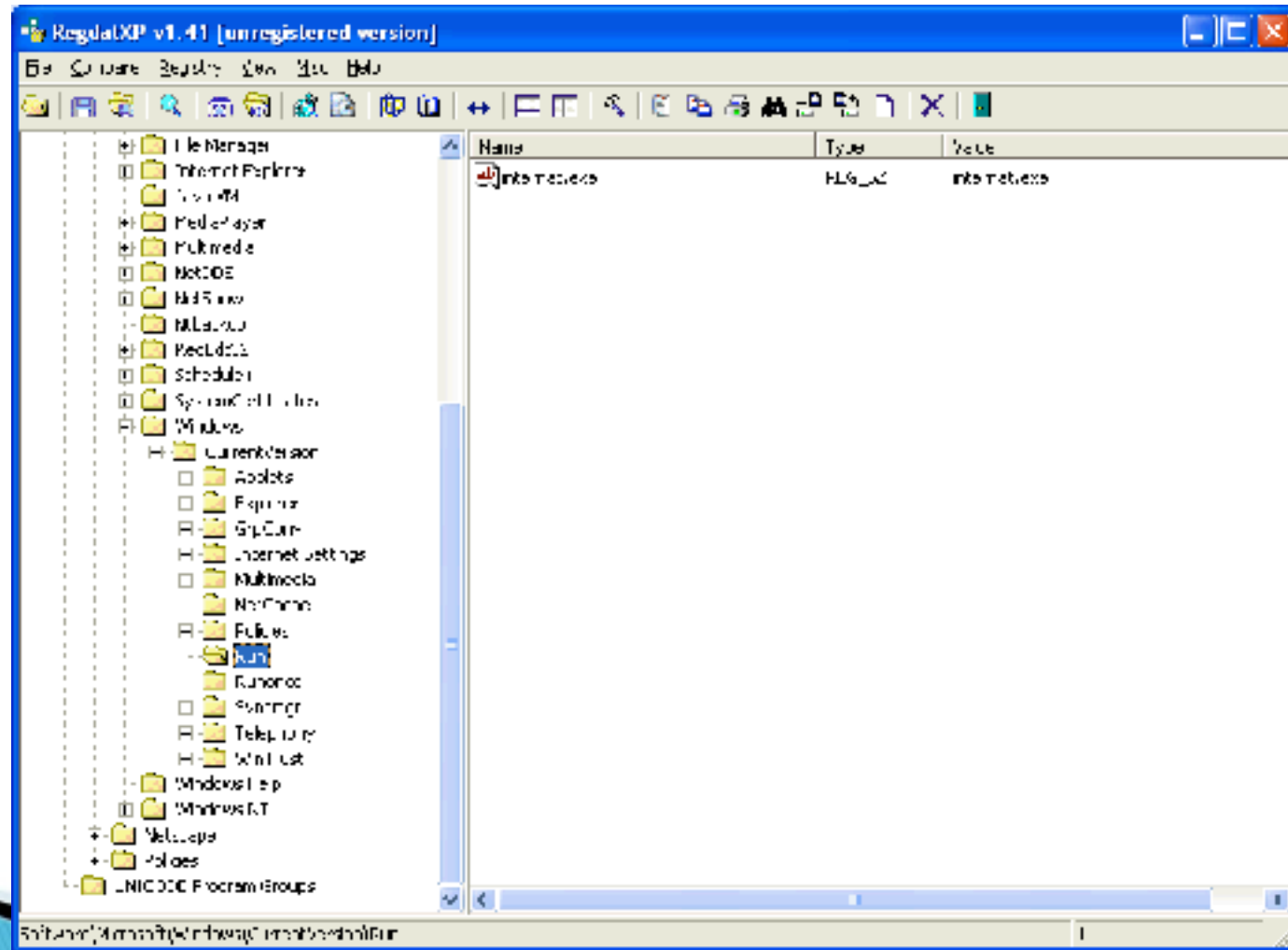
Vulnerability of a critical program in a banking institution (4)



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



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

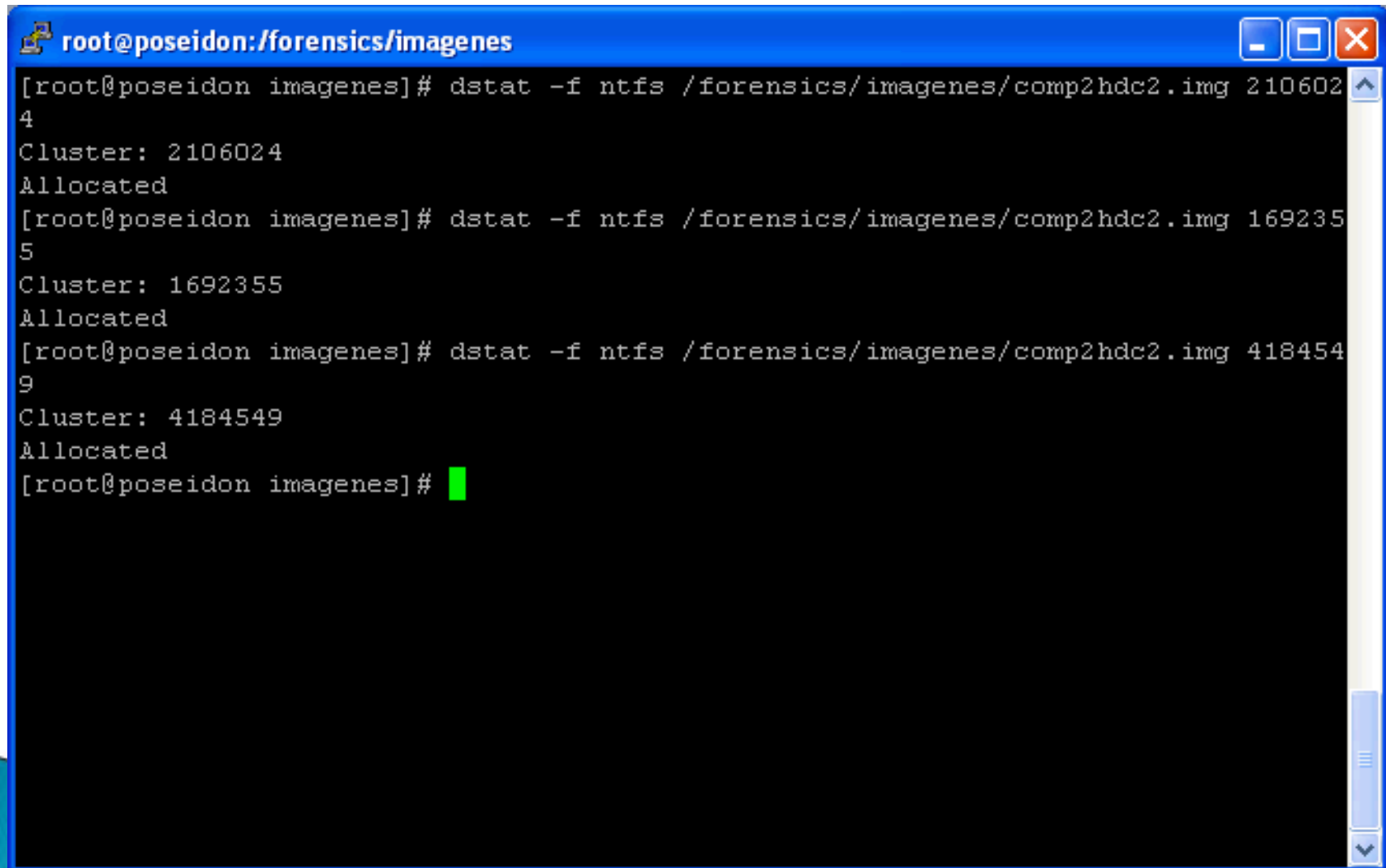


Vulnerability of a critical program in a banking institution (7)

- ▶ 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

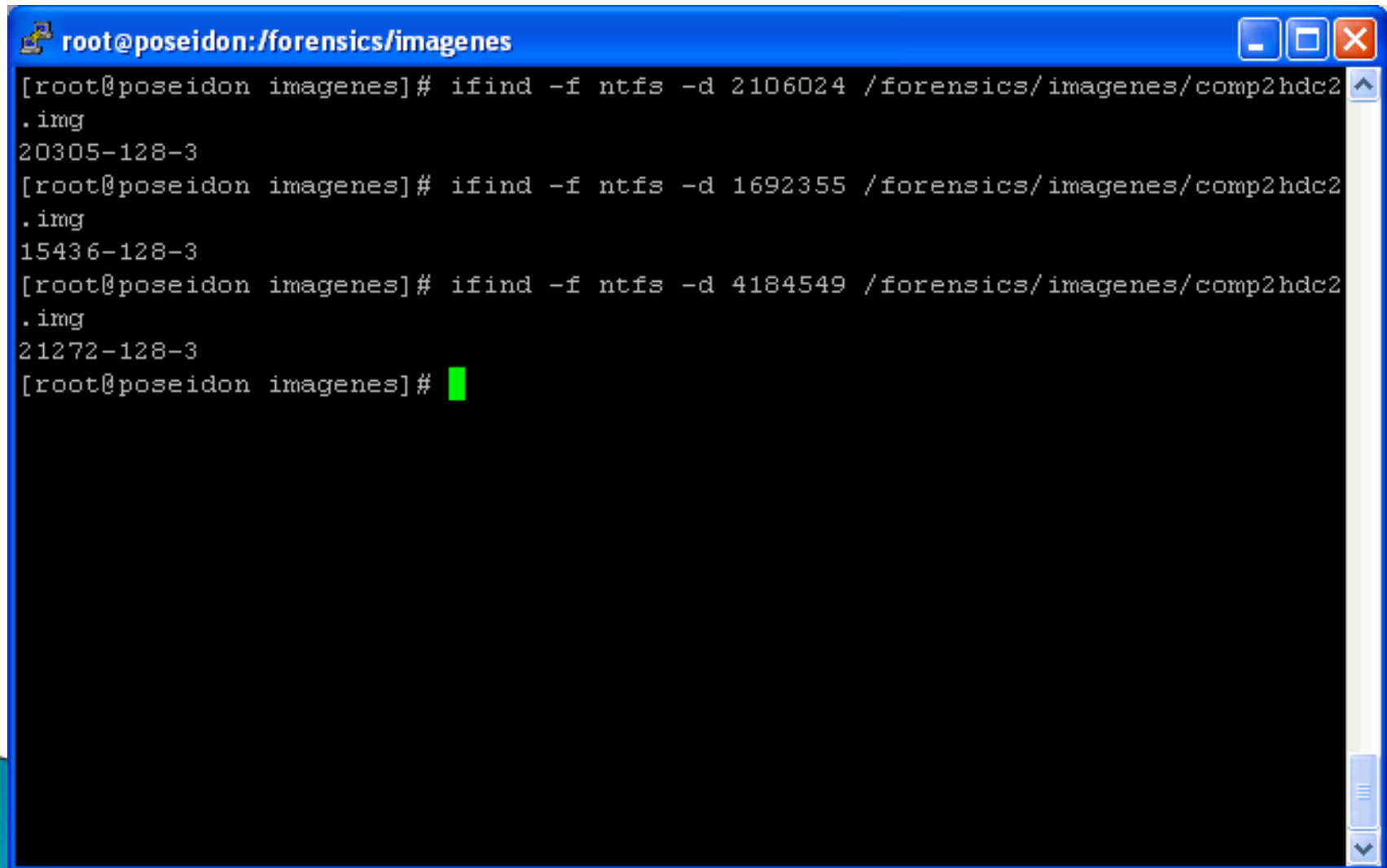


Vulnerability of a critical program in a banking institution (8)



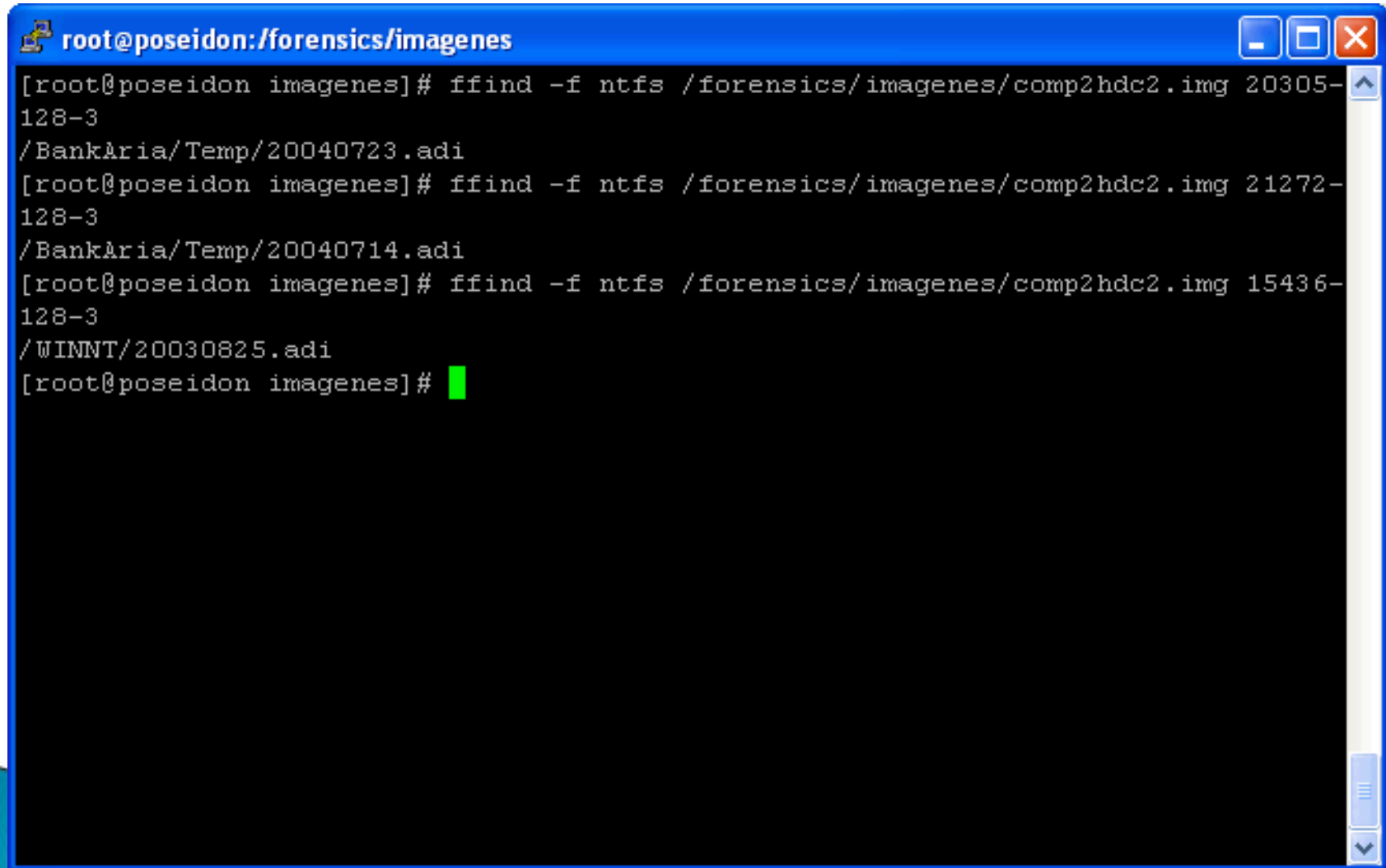
```
root@poseidon://forensics/imagenes  
[root@poseidon imagenes]# dstat -f ntfs /forensics/imagenes/comp2hdc2.img 210602  
4  
Cluster: 2106024  
Allocated  
[root@poseidon imagenes]# dstat -f ntfs /forensics/imagenes/comp2hdc2.img 169235  
5  
Cluster: 1692355  
Allocated  
[root@poseidon imagenes]# dstat -f ntfs /forensics/imagenes/comp2hdc2.img 418454  
9  
Cluster: 4184549  
Allocated  
[root@poseidon imagenes]# █
```

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



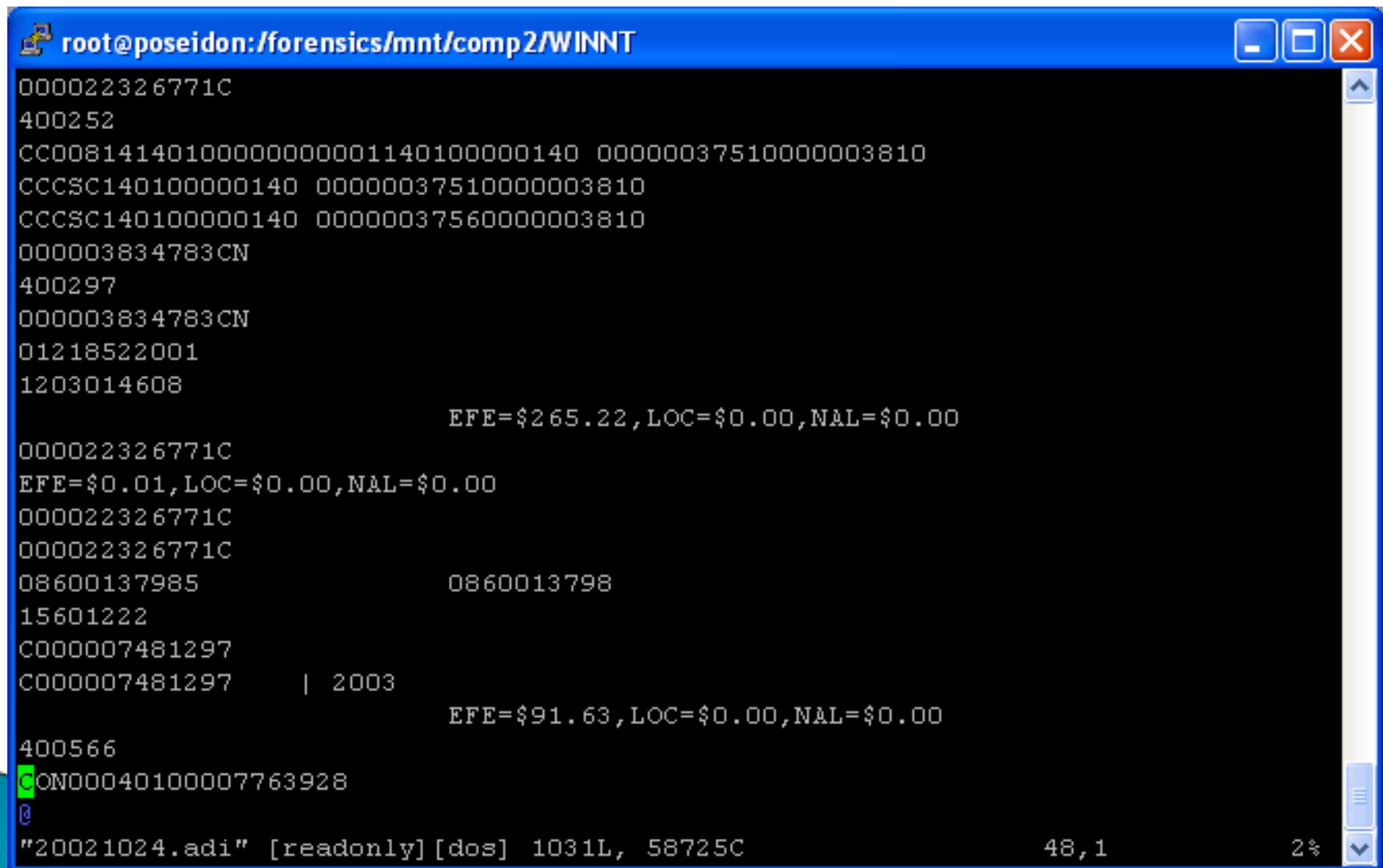
```
root@poseidon://forensics/imagenes
[root@poseidon imagenes]# ifind -f ntfs -d 2106024 /forensics/imagenes/comp2hdc2
.img
20305-128-3
[root@poseidon imagenes]# ifind -f ntfs -d 1692355 /forensics/imagenes/comp2hdc2
.img
15436-128-3
[root@poseidon imagenes]# ifind -f ntfs -d 4184549 /forensics/imagenes/comp2hdc2
.img
21272-128-3
[root@poseidon imagenes]# █
```

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



```
root@poseidon:/forensics/imagenes
[root@poseidon imagenes]# ffind -f ntfs /forensics/imagenes/comp2hdc2.img 20305-128-3
/BankAria/Temp/20040723.adi
[root@poseidon imagenes]# ffind -f ntfs /forensics/imagenes/comp2hdc2.img 21272-128-3
/BankAria/Temp/20040714.adi
[root@poseidon imagenes]# ffind -f ntfs /forensics/imagenes/comp2hdc2.img 15436-128-3
/WINNT/20030825.adi
[root@poseidon imagenes]#
```

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



```
root@poseidon:/forensics/mnt/comp2/WINNT
000022326771C
400252
CC00814140100000000001140100000140 00000037510000003810
CCCSC140100000140 00000037510000003810
CCCSC140100000140 00000037560000003810
000003834783CN
400297
000003834783CN
01218522001
1203014608
                                EFE=$265.22,LOC=$0.00,NAL=$0.00
000022326771C
EFE=$0.01,LOC=$0.00,NAL=$0.00
000022326771C
000022326771C
08600137985                        0860013798
15601222
C000007481297
C000007481297      | 2003
                                EFE=$91.63,LOC=$0.00,NAL=$0.00
400566
C0N00040100007763928
@
"20021024.adi" [readonly] [dos] 1031L, 58725C          48,1          2%
```

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.

