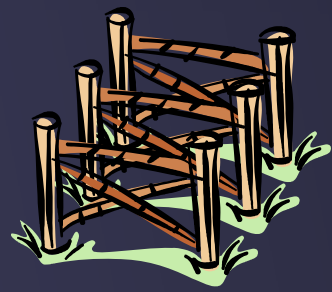
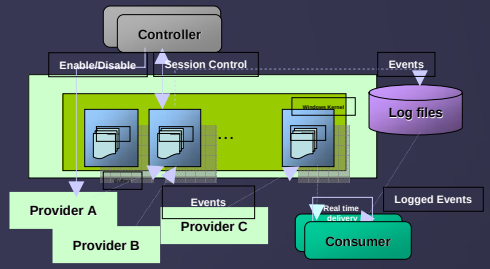
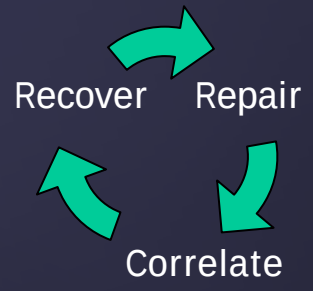
Vista Log Forensics

Dr. Rich Murphey, ACS

- Background
- Case Study
  - Engagement
  - Preliminary Report
  - Final Report
- Vista Event Logging
  - Logging Service
  - Vista Event Encoding
  - Undocumented Internals
- Event Log Analysis
  - Recovery
  - Correlation
  - Interpretation
- Shadow Copy Services







Dedicated to:

BitMonk (HTA/Ad Hoc)

Thanks to:

- Jerlyn Mardis, ACS
- Josh Pennell, IO Active
- Matthew Geiger, CERT

Shouts out to:

- MD5, Caesar
- HTA
- Fednaughty
- DT

Special Thanks To

Sponsor:



- Forensics
  - In-depth Analysis, Expert Witness
- Data Recovery
  - Complex RAID, Exotic File Systems
- Consulting
  - Information Security

This is not:

- Legal Advice
- Suitable for testimony

Experience:

- Rice University
  - Ph.D. Electrical and Computer Engineering
- UTMB Med. School
  - Faculty, Physiology & Biophysics
- Pentasafe Security
  - Chief Scientist
- Applied Cognitive Soln.
  - Chief Scientist
  - Expert Witness
  - CISSP, ACE, EnCE

An Author of:

- GNU Graphics
- Asterisk VOIP



  - See “Authors”
- FreeBSD

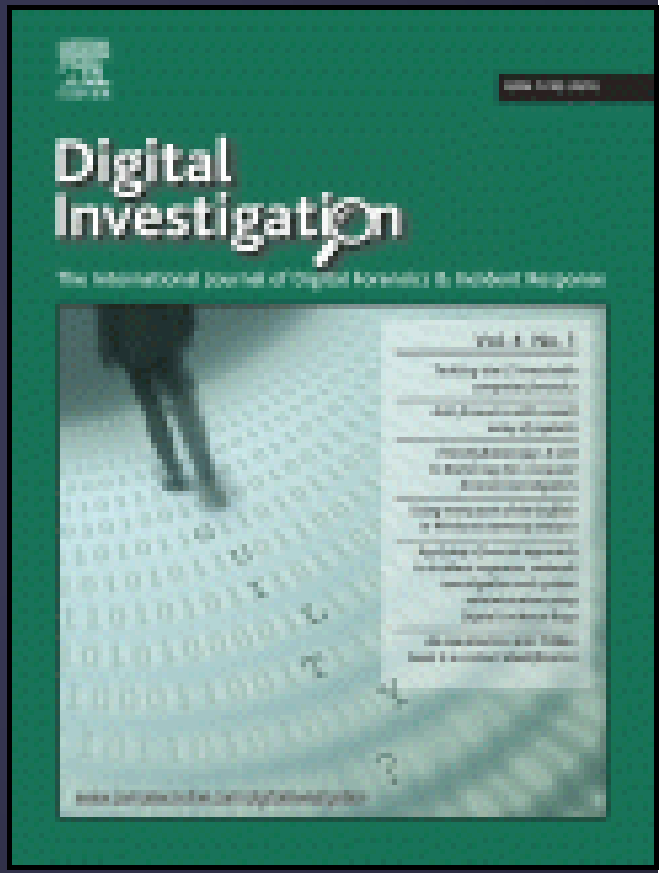


  - Founding Core Team
- XFree86



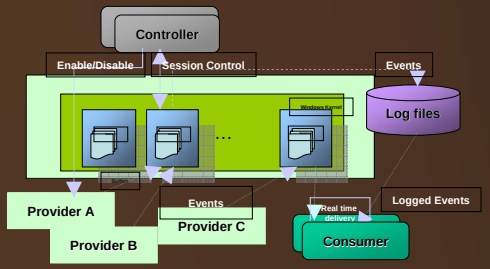
  - man xorg | grep Rich

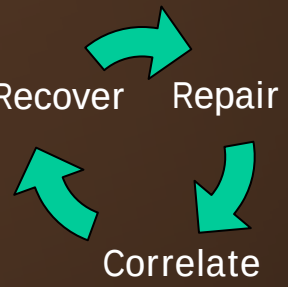
- C. R. Murphey, "Automated Windows Event Log Forensics," Digital Investigation, August 2007
  - A peer-reviewed paper on a new tool for automating XP log recovery and analysis
- Digital Forensic Research Workshop, 8/13/07
- HTCIA National 8/27/07



- Background
- Case Study
  - Engagement
  - Preliminary Results
  - Revised Scope
- Vista Event Logging
  - Events
  - Logging Service
  - Undocumented Internals
- Event Log Analysis
  - Recovery
  - Correlation
  - Report
- Shadow Copy Services

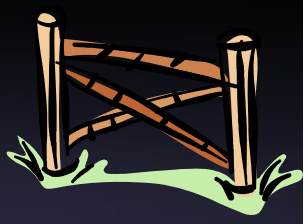






- Step 1: Define Preliminary Scope
  - Define feasibility of the engagement.
- Step 2: Preliminary Report
  - Uncover and mitigate surprises.
  - Define capability to answer questions.
- Step 3: Final Report
  - In-depth coverage.
  - Adapt methods to answer questions.

- Officer/Director calls
  - Something bad happened….
  - Possible contract violation.
  - *Outgoing transfer* of proprietary documents.

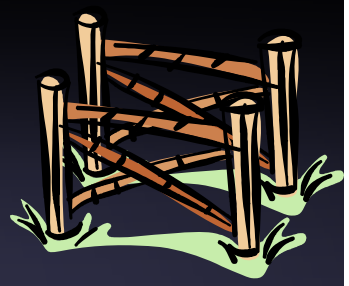


#1: Define a scope of work.

- Can we identify file transfer?
- Examine hard drives
- Email attachments
- File transfer, uploads
- Anything else?



Good news:



- We know what to look for.
- Well defined keywords, file names

#2: Preliminary Report

- D:\OfInterest.doc
- In unallocated space….

Bad News:

- IT deleted the user profile, and gave laptop to a new employee, six months ago, after they reformatted and reinstalled Windows Vista.

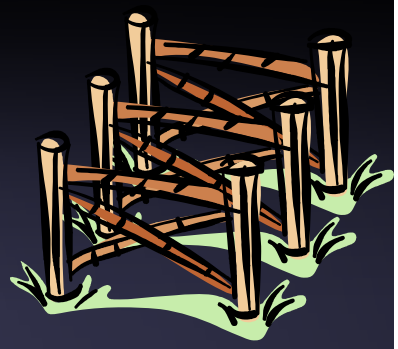


Shortcuts may contain IDs, label, size

- A snapshot of file's attributes, media's attributes

Link target information	
Local Path	D:\OfInterest.doc
Volume Type	CD-ROM
Volume Label	Nov 11 2006
Volume Serial Number	E2C3-F184
File size	1643743
Creation time (UTC)	11/11/2006 3:21:14 PM
Last write time (UTC)	11/3/2006 10:12:34 AM
Last access time (UTC)	N/A
File attributes	
Read-only	

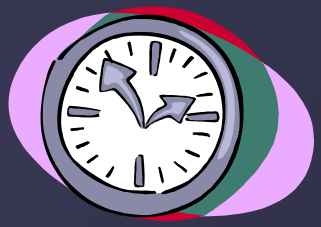
How to identify *outgoing* file transfer?



- Data carve for file path, time….

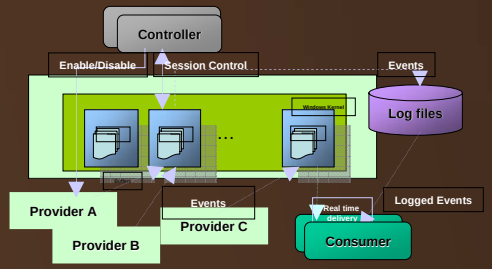
Where to find time stamps?

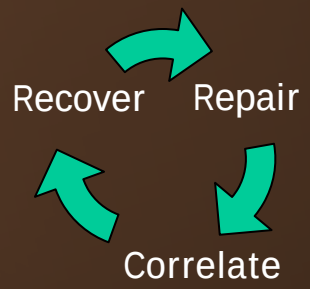
- Event logs
- Internet history
- Shortcuts
- Any where else?



- Background
- Case Study
  - Engagement
  - Preliminary Results
  - Revised Scope
- Vista Event Logging
  - Events
  - Logging Service
  - Undocumented Internals
- Event Log Analysis
  - Recovery
  - Correlation
  - Report
- Shadow Copy Services







Shortcuts may contain IDs, label, size

Shortcut File

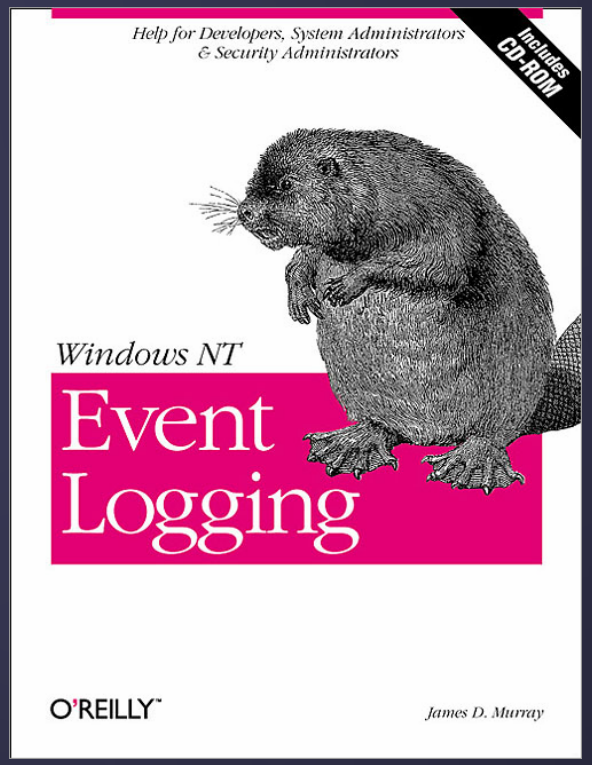
- A snapshot of file's attributes, media's attributes

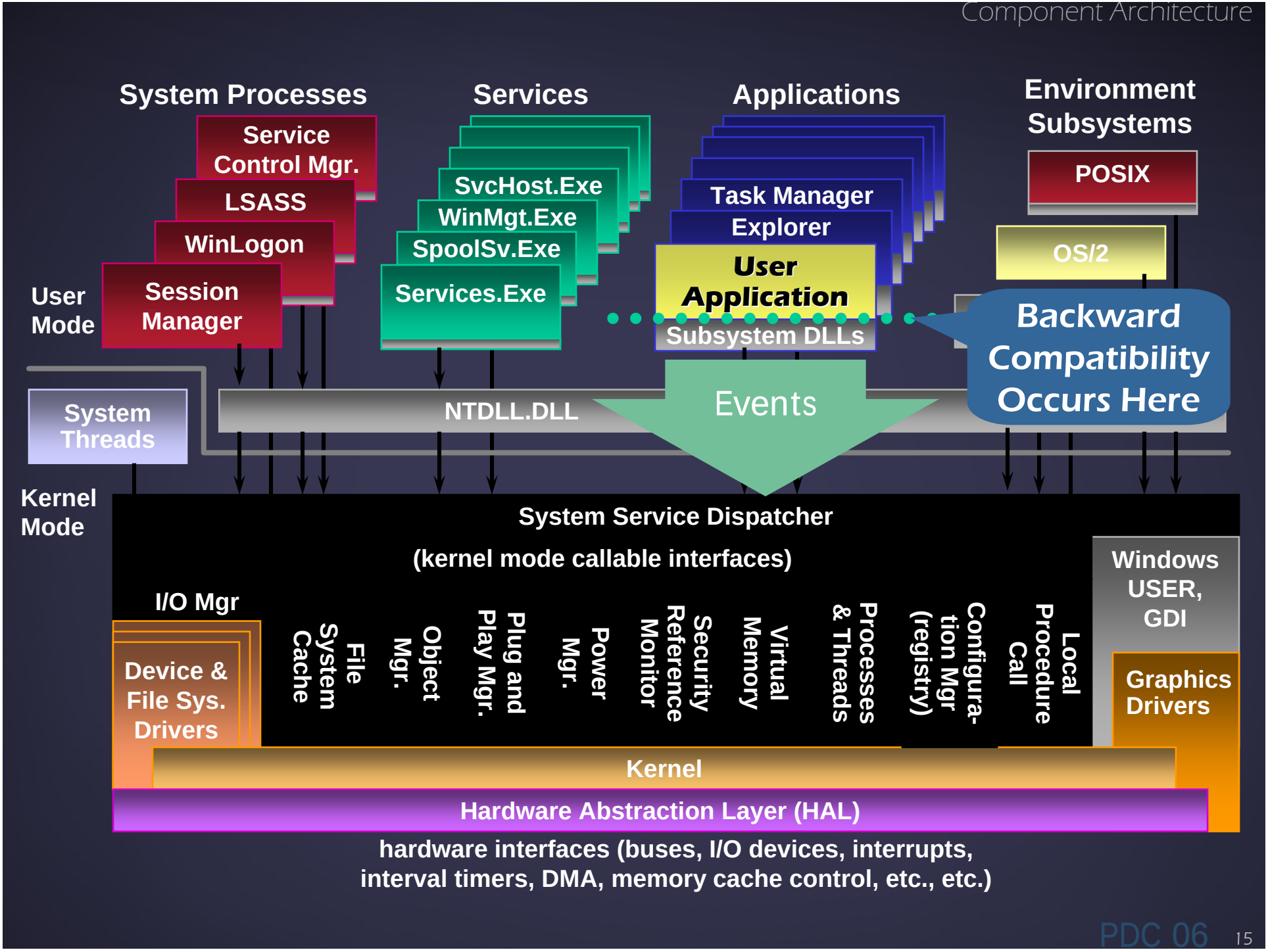
Link target information	
Local Path	D:\OfInterest.doc
Volume Type	CD-ROM
Volume Label	Nov 11 2006
Volume Serial Number	E2C3-F184
File size	1643743
Creation time (UTC)	11/11/2006 3:21:14 PM
Last write time (UTC)	11/3/2006 10:12:34 AM
Last access time (UTC)	N/A
File attributes	
Read-only	

- Windows Vista/2008
  - Time, SID, Source, Severity, Message
  - More than 50 logs by default.

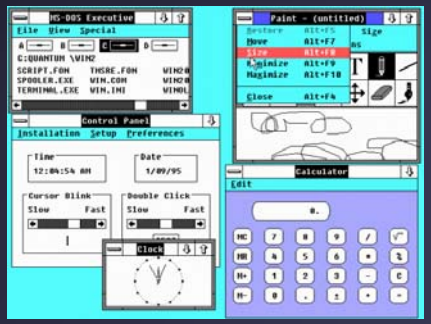
C:/Windows/system32/winevt/Logs/

- Application.evtx
- HardwareEvents.evtx
- Internet Explorer.evtx
- Security.evtx
- Setup.evtx
- System.evtx
- …. 50 more!

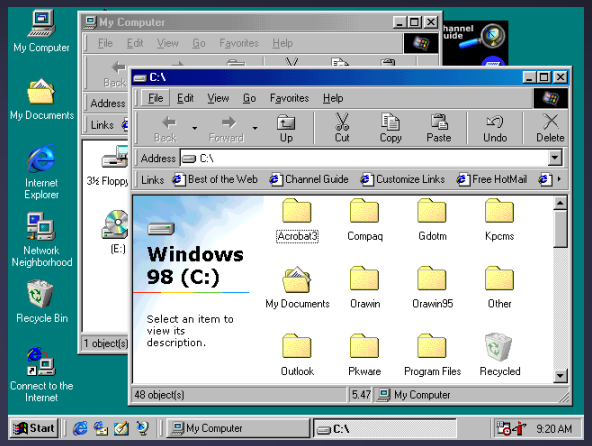



System Processes
Services
Applications
Environment Subsystems
Service Control Mgr.
LSASS
WinLogon
Session Manager
SvcHost.Exe
WinMgt.Exe
SpoolSv.Exe
Services.Exe
Task Manager
Explorer
User Application
Subsystem DLLs
POSIX
OS/2
User Mode
Backward Compatibility Occurs Here
System Threads
NTDLL.DLL
Events
Kernel Mode
System Service Dispatcher
(kernel mode callable interfaces)
I/O Mgr
Device & File Sys. Drivers
File System Cache
Object Mgr.
Plug and Play Mgr.
Power Mgr.
Security Reference Monitor
Virtual Memory
Processes & Threads
Configura-tion Mgr (registry)
Local Procedure Call
Windows USER, GDI
Graphics Drivers
Kernel
Hardware Abstraction Layer (HAL)
hardware interfaces (buses, I/O devices, interrupts,
interval timers, DMA, memory cache control, etc., etc.)

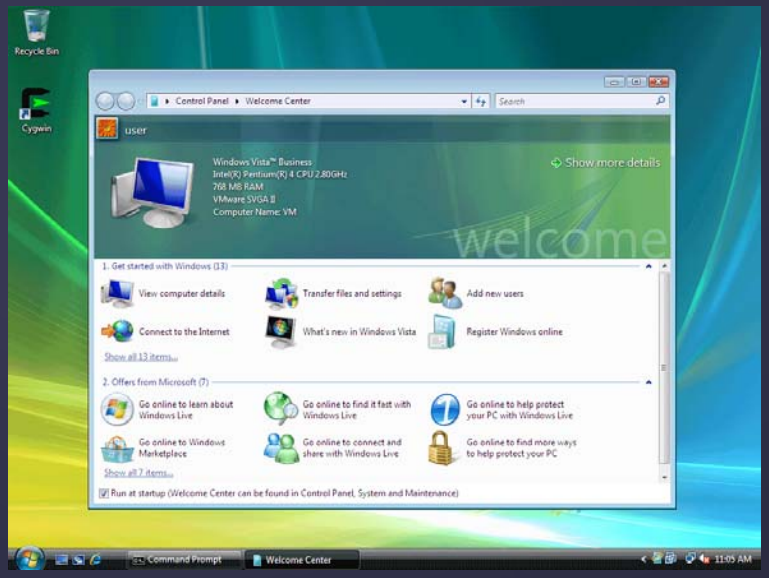
Backward Compatibility?



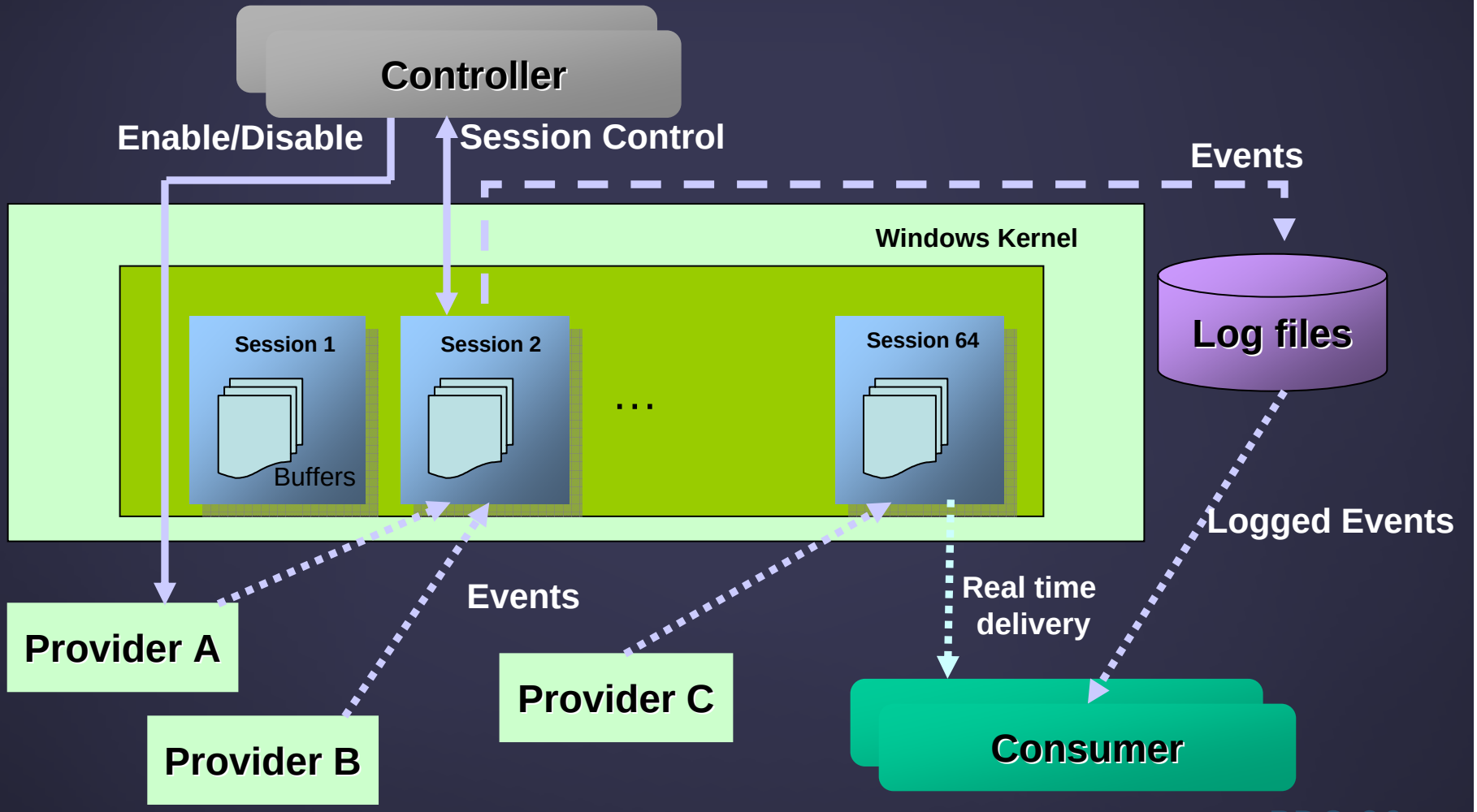




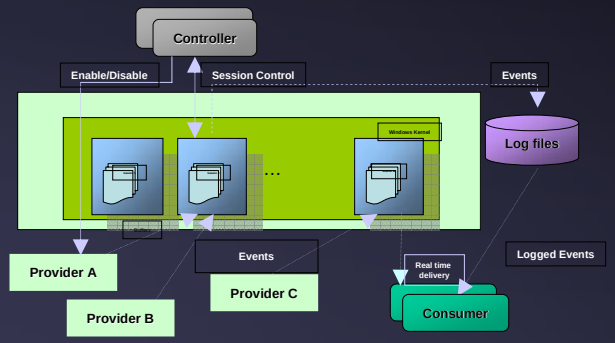




- 5% CPU for 20K events/sec, 200K w/Transactions
- Logging and WMI are now just layers on top of ETW
- Unified: kernel/app, tracing/logging, remote/local



- High performance *tracing*
  - Event Tracing for Windows (ETW)
  - Events from both apps and kernel



- Events are forwarded to a *Collector Service* and stored in local log for consumption
  - Buffered in kernel
  - Dynamically enable/disable
  - No reboot or restart
- Selected events are delivered as they arrive
  - Choose either push or pull subscription

- Events are XML!
  - Standards encoding
  - System: standard properties
  - EventData: app. defined
- Get events via:
  - Query live logs & log files
  - Subscribe to live logs
  - Filter using XPath
- Internals:
  - New, different encoding
  - Arbitrary structure defined by each application

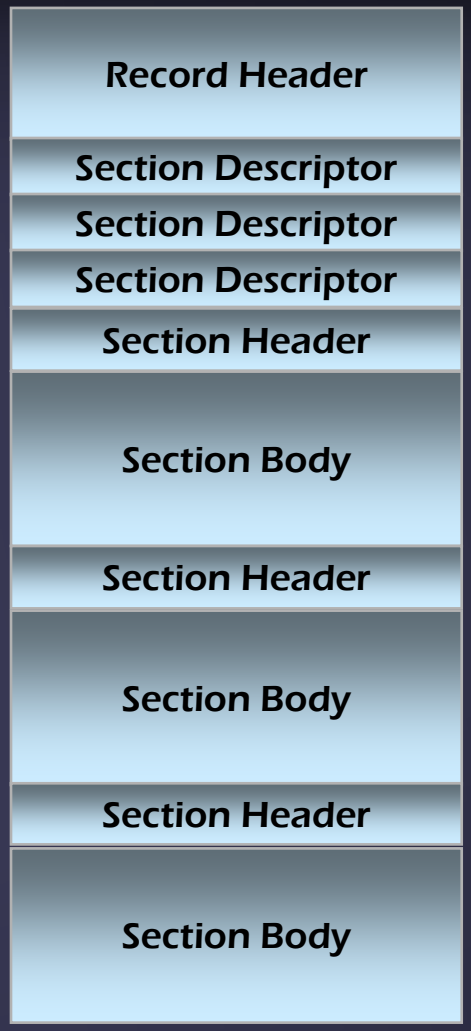
```
<Event>
  <System>
    <Provider Name="CD Burning Service" />
    <EventID>310</EventID>
    <Level>2</Level>
    <Version>0</Version>
    <TimeCreated SystemTime="2006-02-
28T21:51:44.754Z" />
    <EventRecordID>7664</EventRecordID>
    <Channel>Application</Channel>
    <Computer>Desktop9237</Computer>
    <Security UserID="S-1-...-1003" />
  </System>
    <EventData>
        <data name="control">
            Service Started.
        </data>
    </EventData>
</Event>
```

Events are encoded not as XML, but rather BXML!

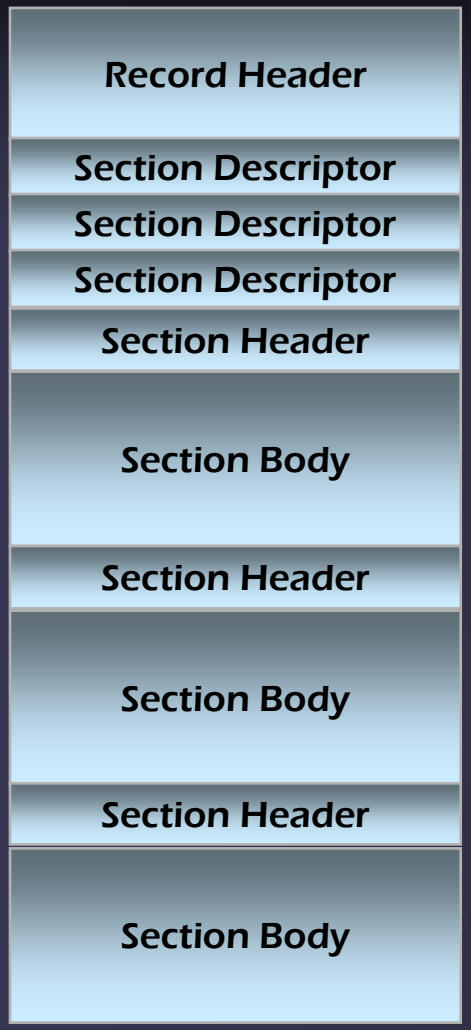
On the outside

```
<Event>
  <System>
    <Provider Name="CD Burning Service" />
    <EventID>310</EventID>
    <Level>2</Level>
    <Version>0</Version>
    <TimeCreated SystemTime="2006-02-
28T21:51:44.754Z" />
    <EventRecordID>7664</EventRecordID>
    <Channel>Application</Channel>
    <Computer>Desktop9237</Computer>
    <Security UserID="S-1-...-1003" />
  </System>
    <EventData>
        <data name=“control”>
            Service Started.
        </data>
    </EventData>
</Event>
```

On the inside



- Record header
  - Common attributes
  - Timestamp, severity
  - Number of sections
- Section descriptors
  - Source
  - Offset, length
- Section headers
  - Specifies encoding of body
- Section body
  - event specific data



- BXML (Binary eXtensible Markup Lang.)
  - A binary *serialization* of an XML document.
  - developed by CubeWerx for OpenGIS Consortium.
  - Higher performance in both space and time.
- More compact.
  - String table for tags and values.
  - Gzip whole doc or just body.
  - Avoids resource exhaustion of DOM.
- 10 to 100 times faster to parse.
  - 100 times faster for dense numeric data due to binary encoding of numbers alone.

- Serialized numbers begins a one byte code that identifies the data type.

```
byte enum ValueType {
    BoolCode = 0xF0,            // boolean value
    ByteCode = 0xF1,            // 'byte' numeric value
    IntCode = 0xF4,             // 'int' numeric value
}

IntNum {                        // 32-bit integer value
    ValueType type = IntCode;
    int num;                    // value
}
```

- XML tags are serialized as a byte code for the type of tag, followed by a reference to the tag name in the string table.

```
ContentElementToken {          // <element>
    TokenType type = ContentElementCode;
    Count stringRef;           // index of
  element name
}

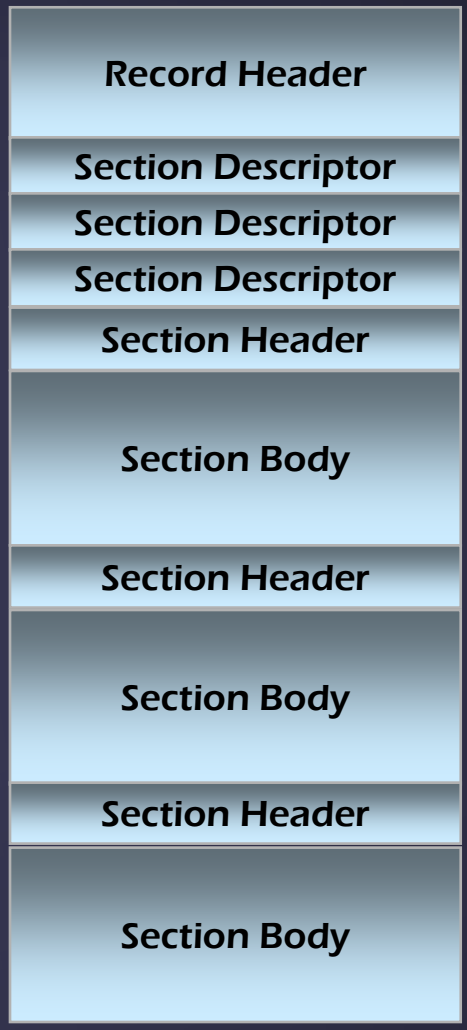
ElementEndToken {              // </element>
    TokenType type = ElementEndCode;
}
```

- Strings are preceeded by their length.
- String tables are preceeded by type code and table size.

```
String {                                  // raw character string
  Count byteLength;          // length in bytes
  byte chars[byteLength]; // characters in proper encoding
}

StringTableToken {                 // string table (fragment)
  TokenType type = StringTableCode;
  Count nStrings;                 // number of strings
  String strings[nStrings]; // values
}
```

- Performance, scalability, and security
- New event publishing API
  - Schematized, discoverable, structured events
  - Unified API
    - logging uses tracing framework
  - Logging is asynchronous
    - Does not block the application
- Log size limit removed
  - limited only by disk space



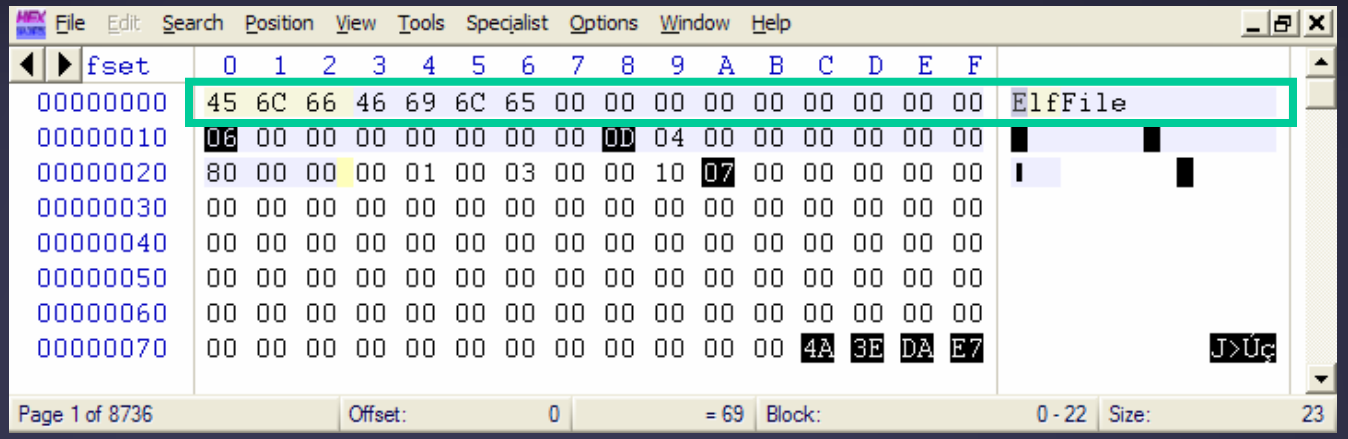
- XML events have *rich* information
  - XP Events have flat structure, no parameter names
- Filtering and Subscriptions – XPath
  - Event[System/EventID=101]
- Select events - filter out noise

```
<QueryList>
  <Query>
    <Select>Event[System/Provider=Foo]</Select>
    <Suppress>Event[System/Level>2]</Suppress>
  </Query>
</QueryList>
```

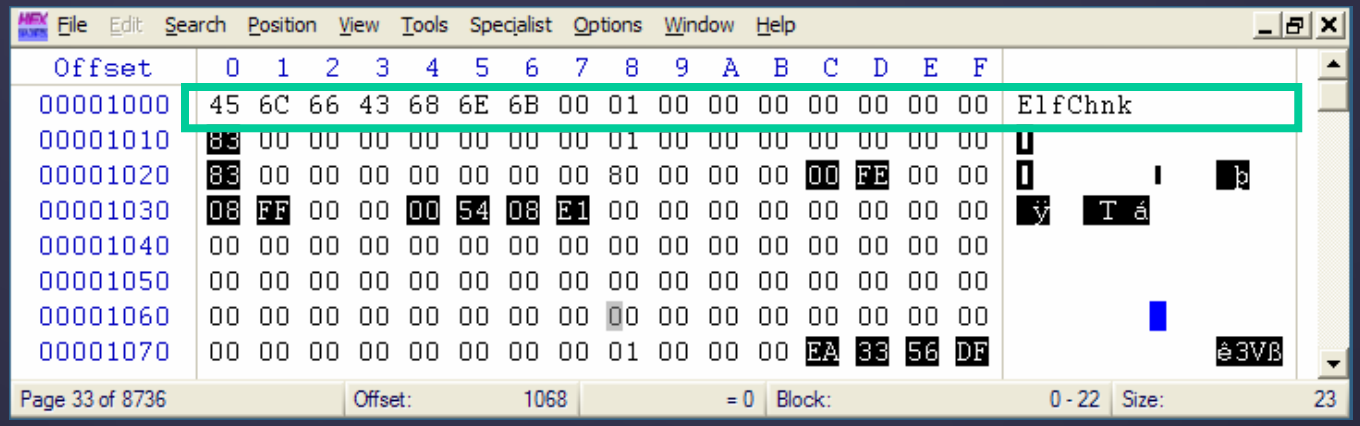
- Filter across live logs, files, Vista, and XP
  - Subscribe to a custom view of events centrally
  - Integrates with existing tools
- Triggering Actions
  - Associate a task with an event with a single click

Vista Log Signature

- 4K Header starts with “ElfFile”



- Each 64K block starts with “ElfChnk”



- Size: 1024 + 4 = 1028 K bytes

- Providers are sources of the events
- Identified by unique GUID and name
- Specifies the location of resources for decoding

```
<provider name="Microsoft-Windows-Demonstration"
                guid="{12345678-d6ef-4962-83d5-123456789012}“
                resourceFileName="wevtsvc.dll"
                messageFileName="wevtsvcMessages.dll"
                parameterFileName="wevtsvcParameter.dll"
>
```

- System-defined channels are imported (System channel above)
- New provider-specific channels can be defined and configured

```
<importChannel chid="C1" name="System" />
<channel chid="C2" name="Microsoft-Windows-
  Demonstration/Operational“
                type="Operational" isolation="System">
    <logging>
        <autoBackup>true</autoBackup>
        <maxSize>268435456</maxSize>
    </logging>
    <publishing>
        <level>2</level>
        <keywords>1</keywords>
    </publishing>
</channel>
```

- Templates define the payload shape of events
- Data elements define fields of events
- Can add user-defined XML representation for the payload

```
<templates>
  <template tid="tid_HelloWorld">
    <data name="Greeting" inType="win:UnicodeString"
 outType="xs:string" />
  </template>
</templates>
```

- Manifest defines event attributes: ID (value), version, keywords, task, opcode, and level
- References previously declared template that defines instance data
- Message - a user readable string
- Channel - the name of the channel that transports the event to logs

```
<event value="101" version="1" level="win:Error"
            symbol=“MyEventDescriptor”
            keywords="el:Availability“
            task="el:EventProcessing"
            template=“tid_HelloWorld" channel=“C1"
            message="$(string.HelloWorld.Message)"
/>
```

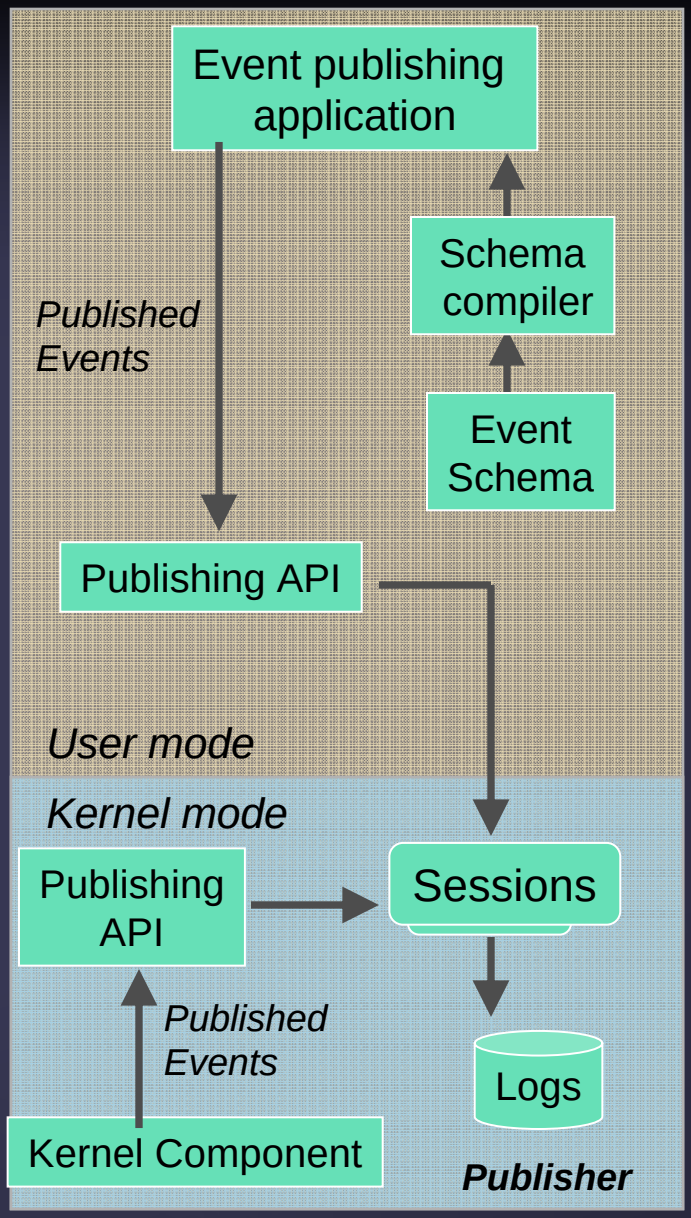
How to log an event:

At compile time

- Write a schema
- Compile schema

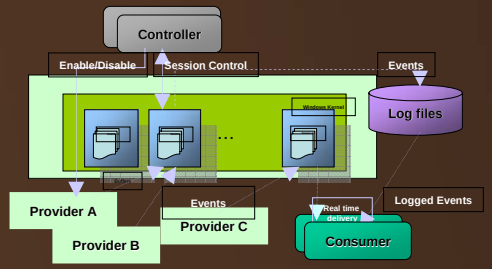
At run time

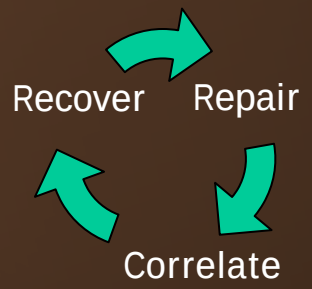
- Register source
- Create a session
- Send events



- Background
- Case Study
  - Engagement
  - Preliminary Results
  - Revised Scope
- Vista Event Logging
  - Events
  - Logging Service
  - Undocumented Internals
- Event Log Analysis
  - Recovery
  - Correlation
  - Report
- Shadow Copy Services

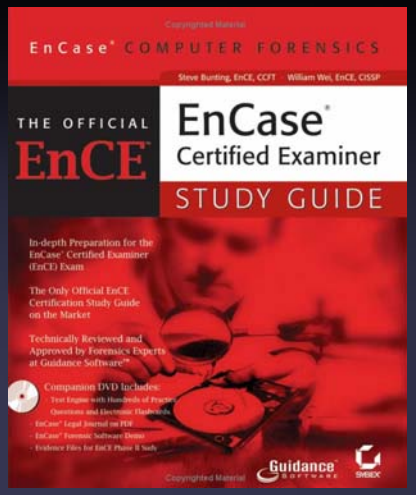






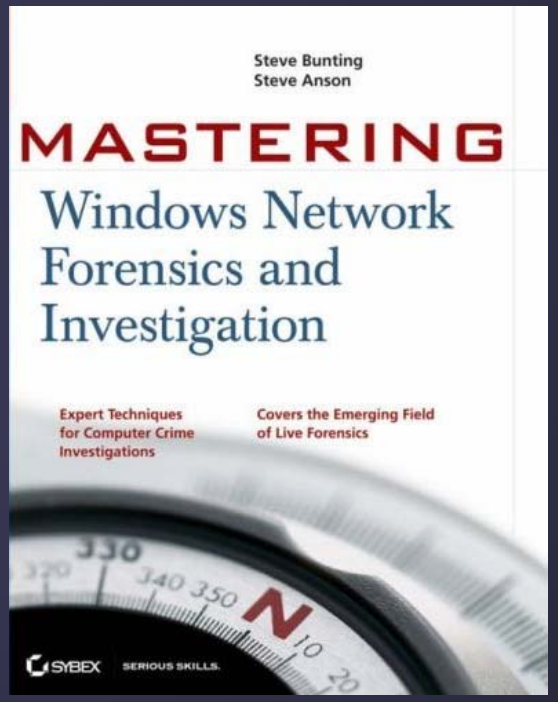
"Conduct Cutting-Edge Forensic Investigations"

– back cover



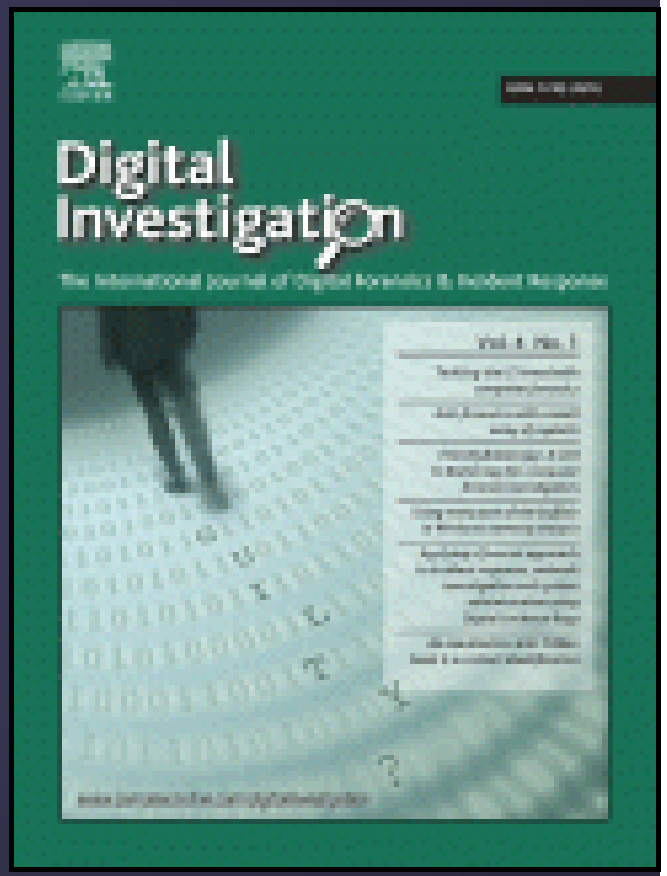
On Event Log Repair:

- "We found no methods that were complete, and none explained the underlying principles for why the repair was needed." – pg. 444

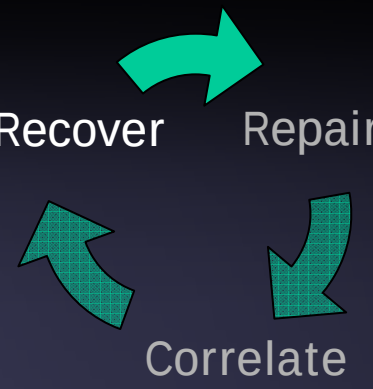


Available April 2, 2007

- C. R. Murphey, "Automated Windows Event Log Forensics," Digital Investigation, August 2007
  - A peer-reviewed paper on a new tool for automating XP log recovery and analysis
- Digital Forensic Research Workshop, 8/13/07
- HTCIA National 8/27/07



Forensic Process Models

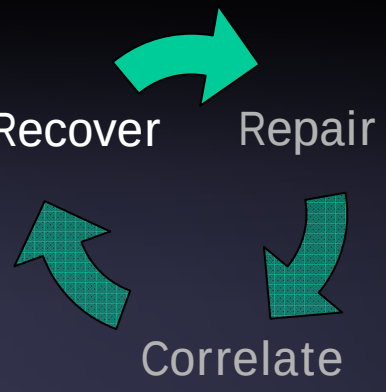


Extract

Analyze

Interpret

Forensic Process Models



Extract:

Step 1 – Recover
- Data Carve for Logs, etc.

Step 2 – Validate
- Identify intact log files.

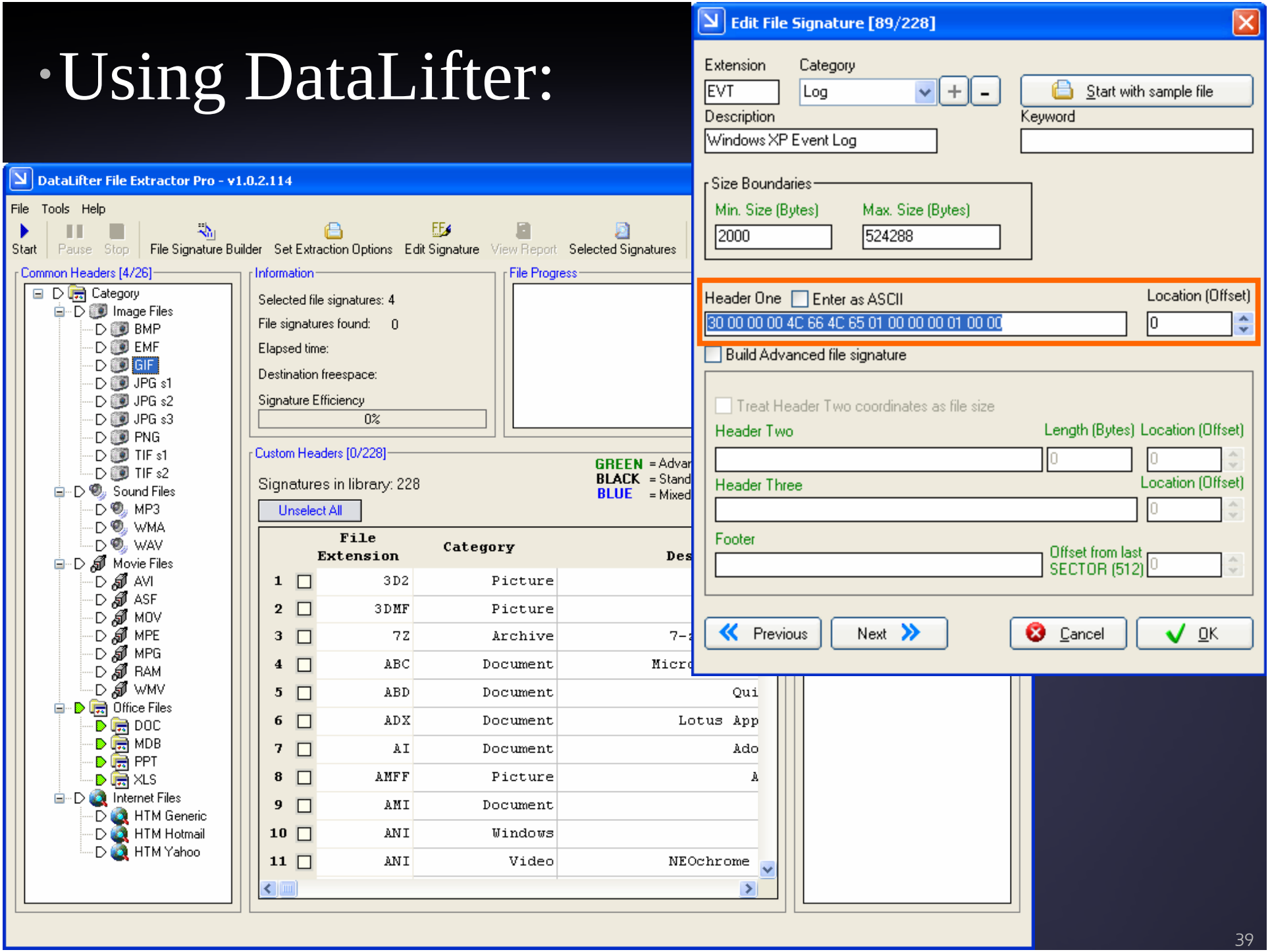
Step 3 – Correlate
- Corresponding time, files, names,…



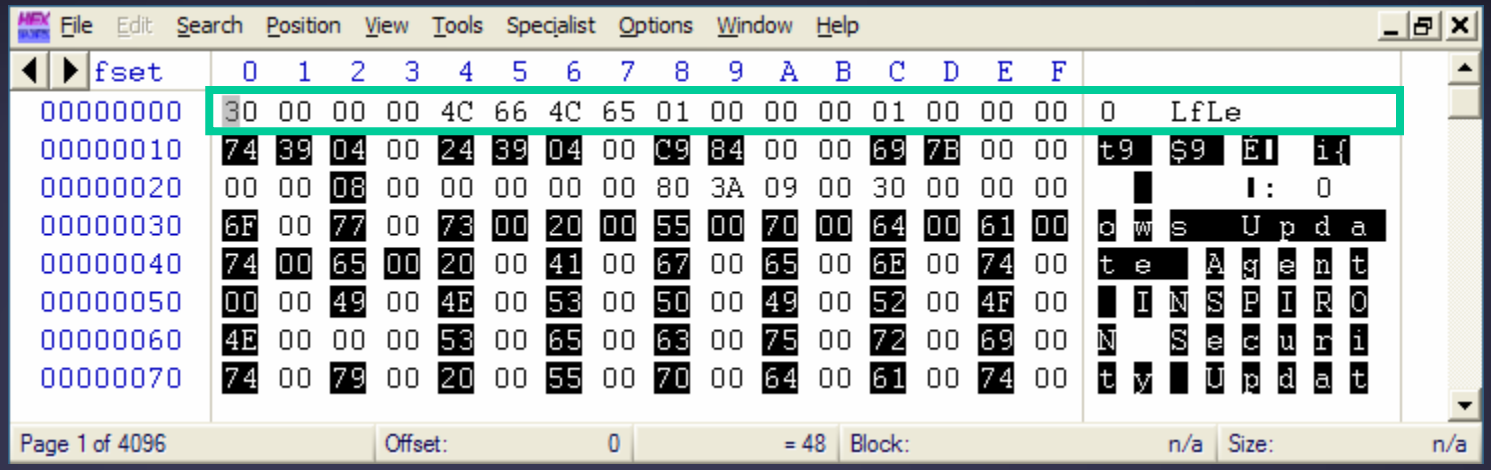
Analyze

Interpret

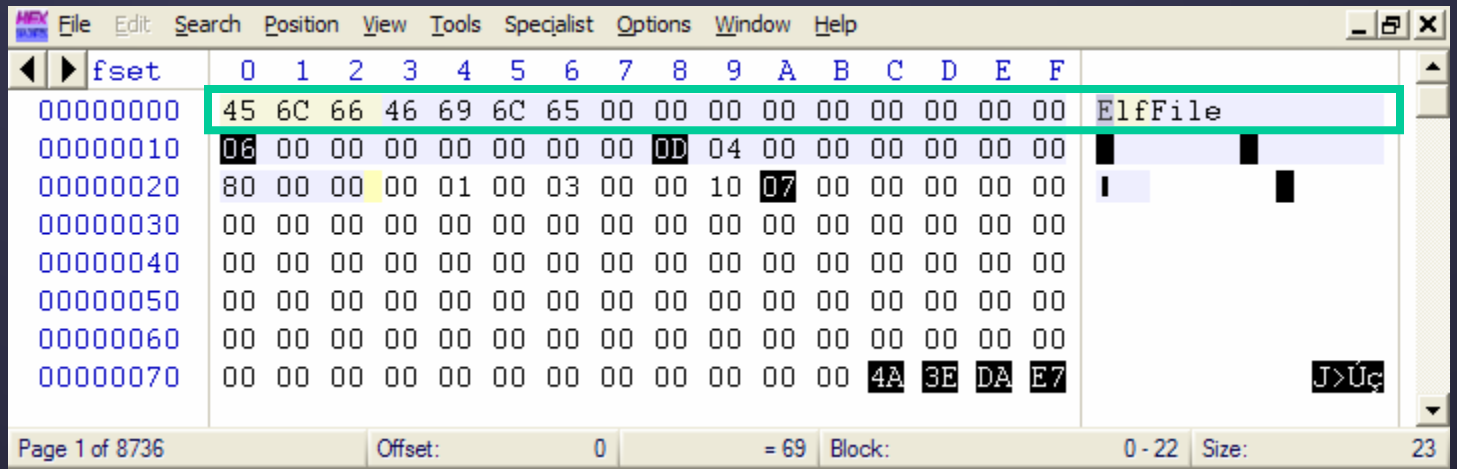
Using DataLifter:



- XP log signature – 16 bytes
  - 30 00 00 00 4c 66 4c 65 01 00 00 00 01 00 00 00

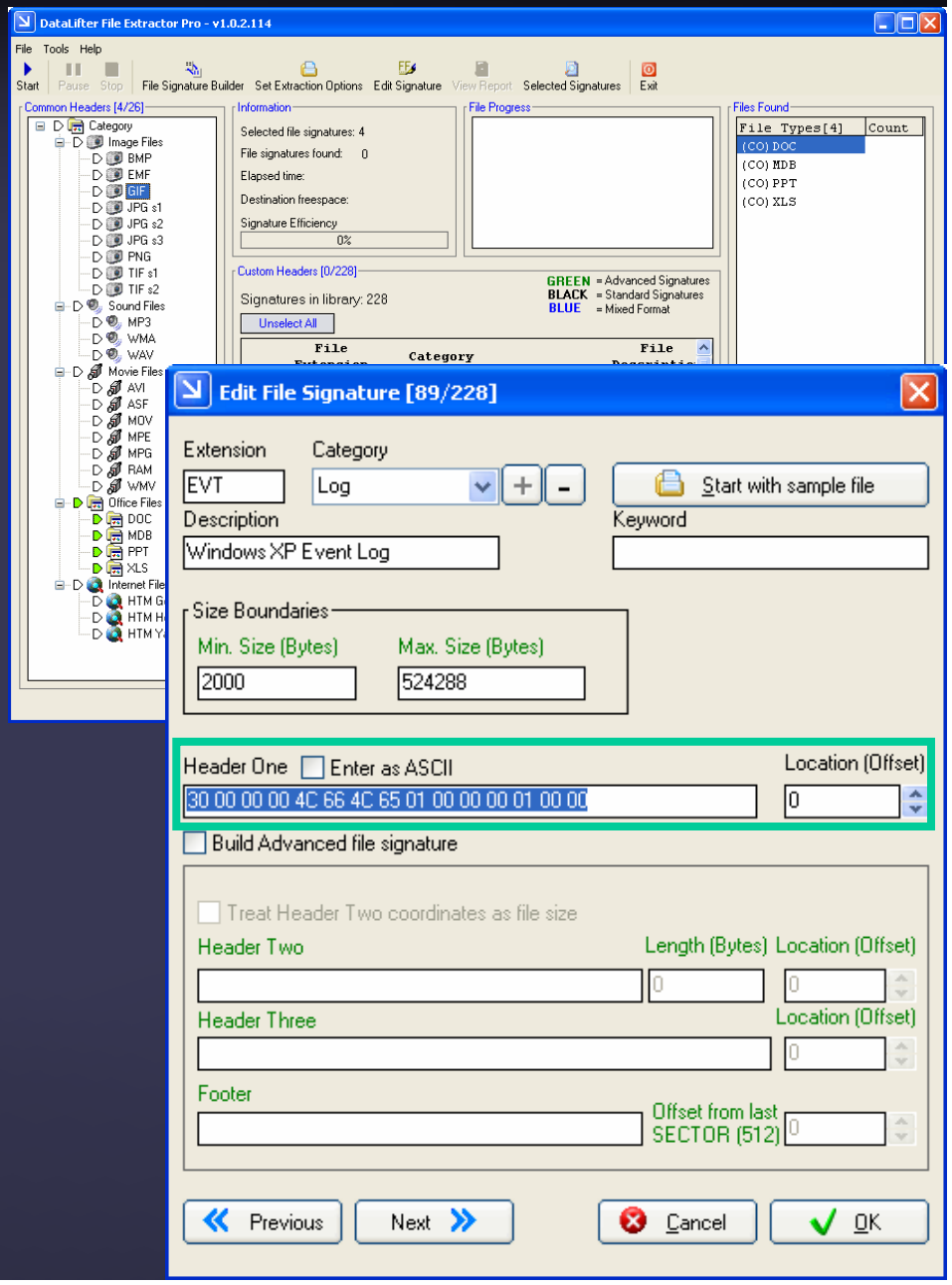


- Vista log signature – 16 bytes
  - "**ElfFile**" padded with nulls

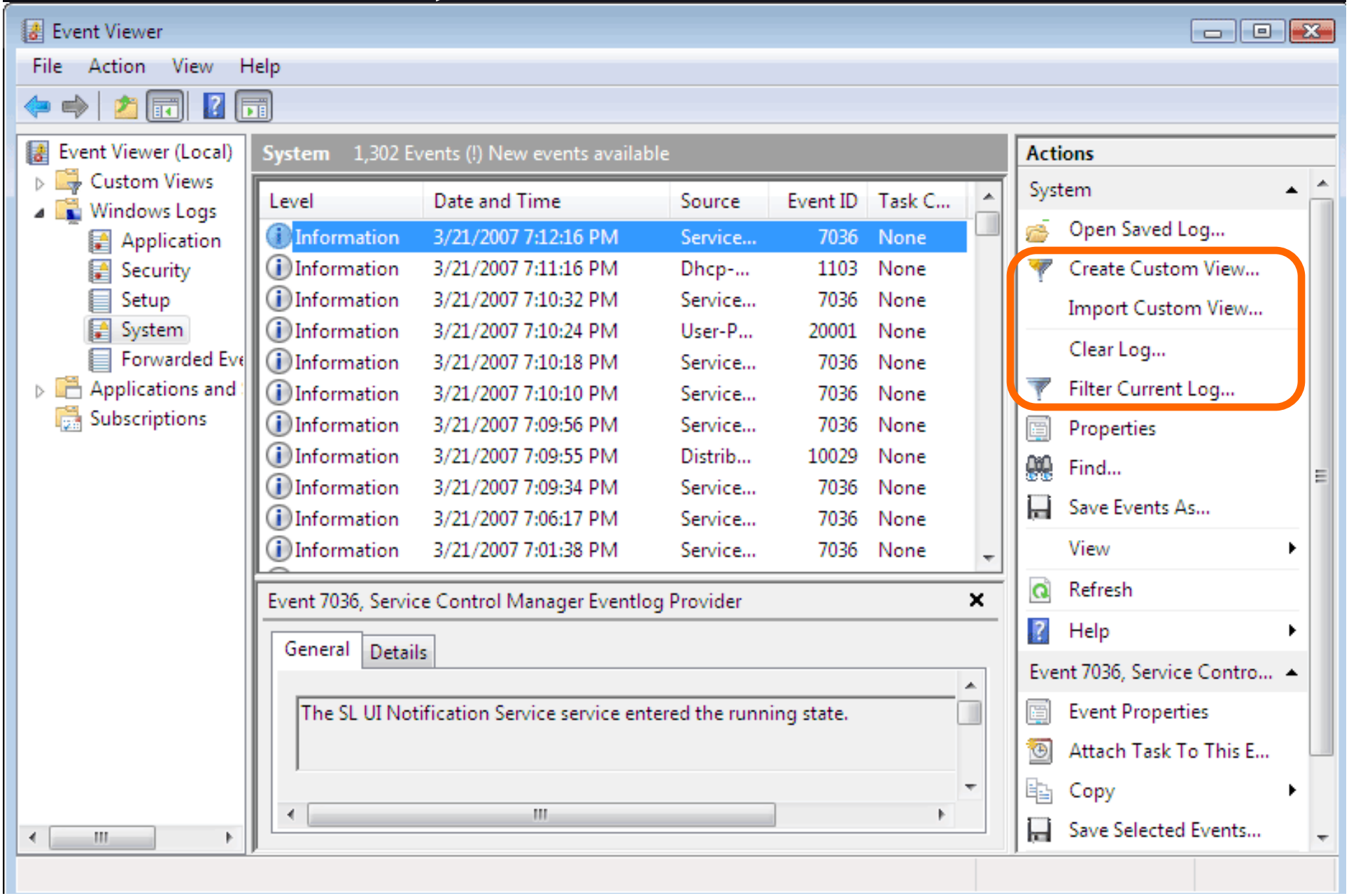


The Results:

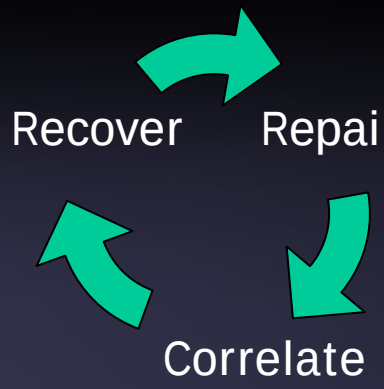
- Step 1 – Recover
  - Run DataLifter
  - 100 logs are recovered.
  - Only two are viewable.
  - 98 corrupt logs
- Step 2
  - Validate 98 logs?



New: Views, Filters



SQL queries to identify patterns




```
<QueryList>
  <Query>
    <Select Path="System">
*[System/Provider="CD Burning Service"]</Select>
  </Query>
</QueryList>
```

Time (UTC)	Message
11/11/2006 15:21	The CD Burning service was successfully sent a start control.
11/11/2006 15:21	The CD Burning service entered the running state.
11/11/2006 15:22	The CD Burning service entered the running state.
11/11/2006 15:23	The CD Burning service entered the running state.
11/11/2006 15:24	The CD Burning service entered the running state.
11/11/2006 15:25	The CD Burning service entered the running state.
11/11/2006 15:26	The CD Burning service entered the running state.
11/11/2006 15:27	The CD Burning service entered the running state.
11/11/2006 15:27	The CD Burning service entered the stopped state.

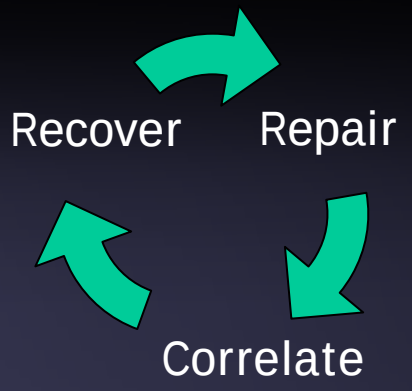
Shortcuts may contain IDs, label, size

Shortcut File

- A snapshot of file's attributes, media's attributes

Link target information	
Local Path	D:\OfInterest.doc
Volume Type	CD-ROM
Volume Label	Nov 11 2006
Volume Serial Number	E2C3-F184
File size	1643743
Creation time (UTC)	11/11/2006 3:21:14 PM
Last write time (UTC)	11/3/2006 10:12:34 AM
Last access time (UTC)	N/A
File attributes	
Read-only	

Correlations indicate



- A CD-ROM was burned
  - By username: Bob
  - At: 11/11/2006 3:21 PM UTC
- We can uniquely identify the CD
  - Label: “Nov 11 2006”
  - Volume serial number: E2C3-F184
- Proprietary documents were transferred.
  - OfInterest.doc, 1.6Mb
  - Last Modified 11/3/2006 10:12:34 AM UTC

Shortcuts may contain IDs, label, size

Shortcut File

- A snapshot of file's attributes, media's attributes

Link target information	
Local Path	D:\OfInterest.doc
Volume Type	CD-ROM
Volume Label	Nov 11 2006
Volume Serial Number	E2C3-F184
File size	1643743
Creation time (UTC)	11/11/2006 3:21:14 PM
Last write time (UTC)	11/3/2006 10:12:34 AM
Last access time (UTC)	N/A
File attributes	
Read-only	

Link target information	
Local Path	D:\OfInterest.doc
Volume Type	CD-ROM
Volume Label	Nov 11 2006
Volume Serial Number	E2C3-F184
File size	1643743
Creation time (UTC)	11/11/2006 3:21:14 PM
Last write time (UTC)	11/3/2006 10:12:34 AM
Last access time (UTC)	N/A
File attributes	
Read-only	

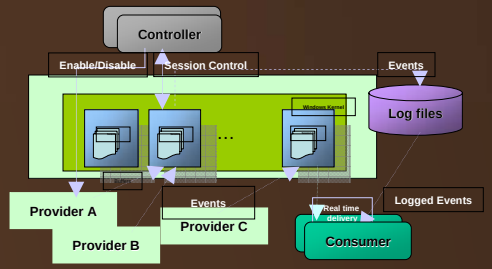
- Last write time is earlier than created.

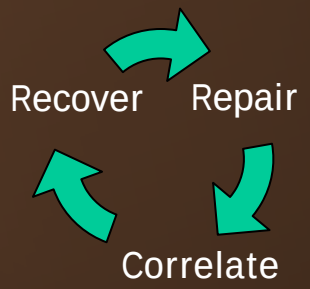
Created	**11/11/2006 3:21:14 PM**
Last write	**11/3/2006 10:12:34 AM**

- Can indicate the time at which a file was transferred from source media.
- Can help identify the source file on source media.

- Background
- Case Study
  - Engagement
  - Preliminary Results
  - Revised Scope
- Vista Event Logging
  - Events
  - Logging Service
  - Undocumented Internals
- Event Log Analysis
  - Recovery
  - Correlation
  - Report
- Shadow Copy Services

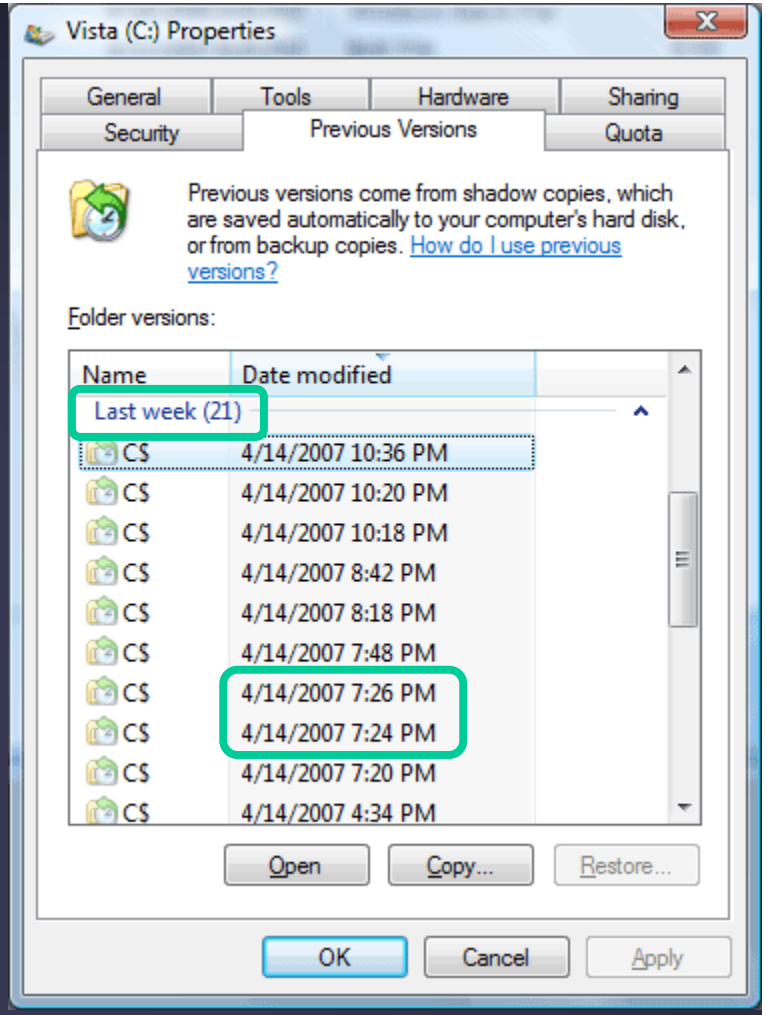






"Shadow Copy tracks your every change."

- Automatic point-in-time copies.
- Incremental block level differences minimize space.
- Deletes older copies as needed for space (LRU).





Revised Federal Rules of Civil Procedure

- Scope of Production
  - Historical snapshots are readily available in Vista
- Duty to Preserve
  - Litigation Hold Notices
  - Potential for Sanctions
- Form of Production
  - Native files?
  - Metadata?
  - Point-in-time Image Snapshots?

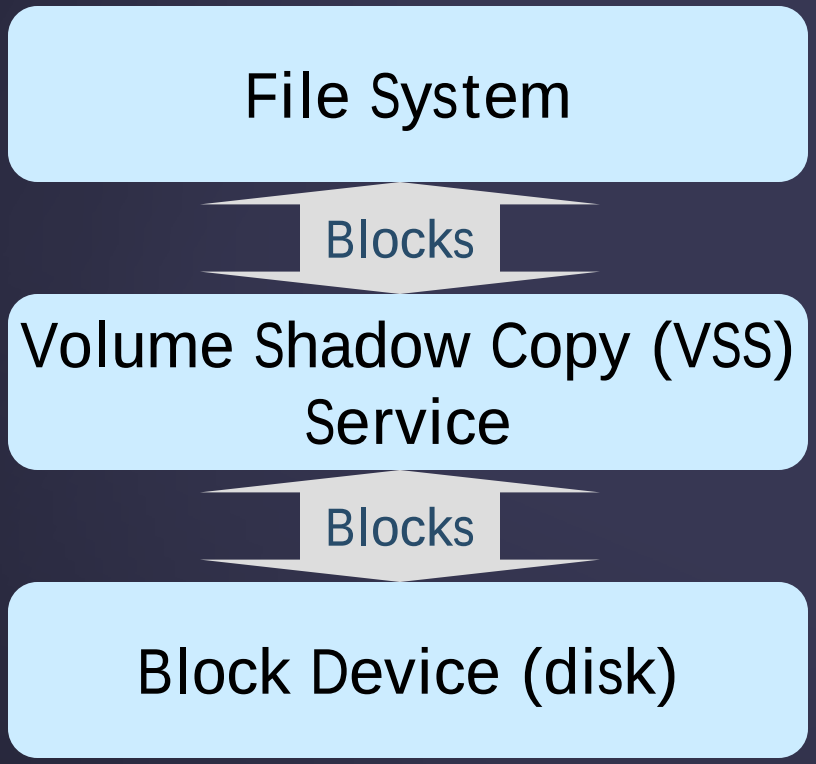
- May Complicate Corporate Policy Issues
- Document retention policies
  - Complicates policy maintenance
  - Disabling shadow copies in turn breaks backups, restore engine
- Metadata retention policy
  - Ownership changes are visible now
  - Gaps in documentation policy for Vista

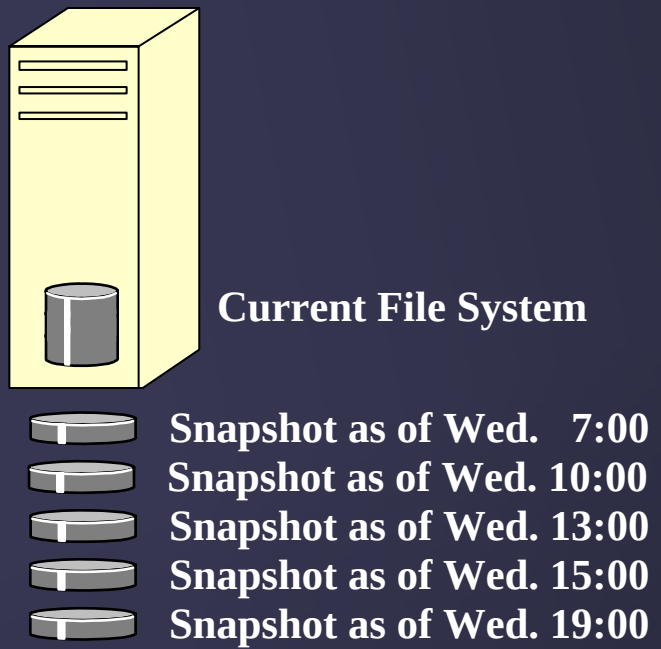
- FRCP: The rules have changed.
- Vista, in turn, changes the rules.

- What happens if one accepts the default system behavior?
  - Things may never go away permanently.
- Vista leaves far more information than XP
  - Changes in ownership (SID)

- Executives dislike surprises
  - Risks regarding SOX compliance and litigation.

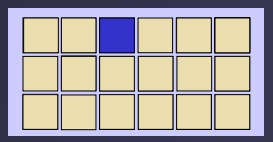
- Acts like block device
- A layer between the device and file system





Shadow Copies

Application writes data to disk

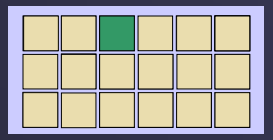


Disk Before

Upon write, overwritten block moves to shadow copy



Shadow Before



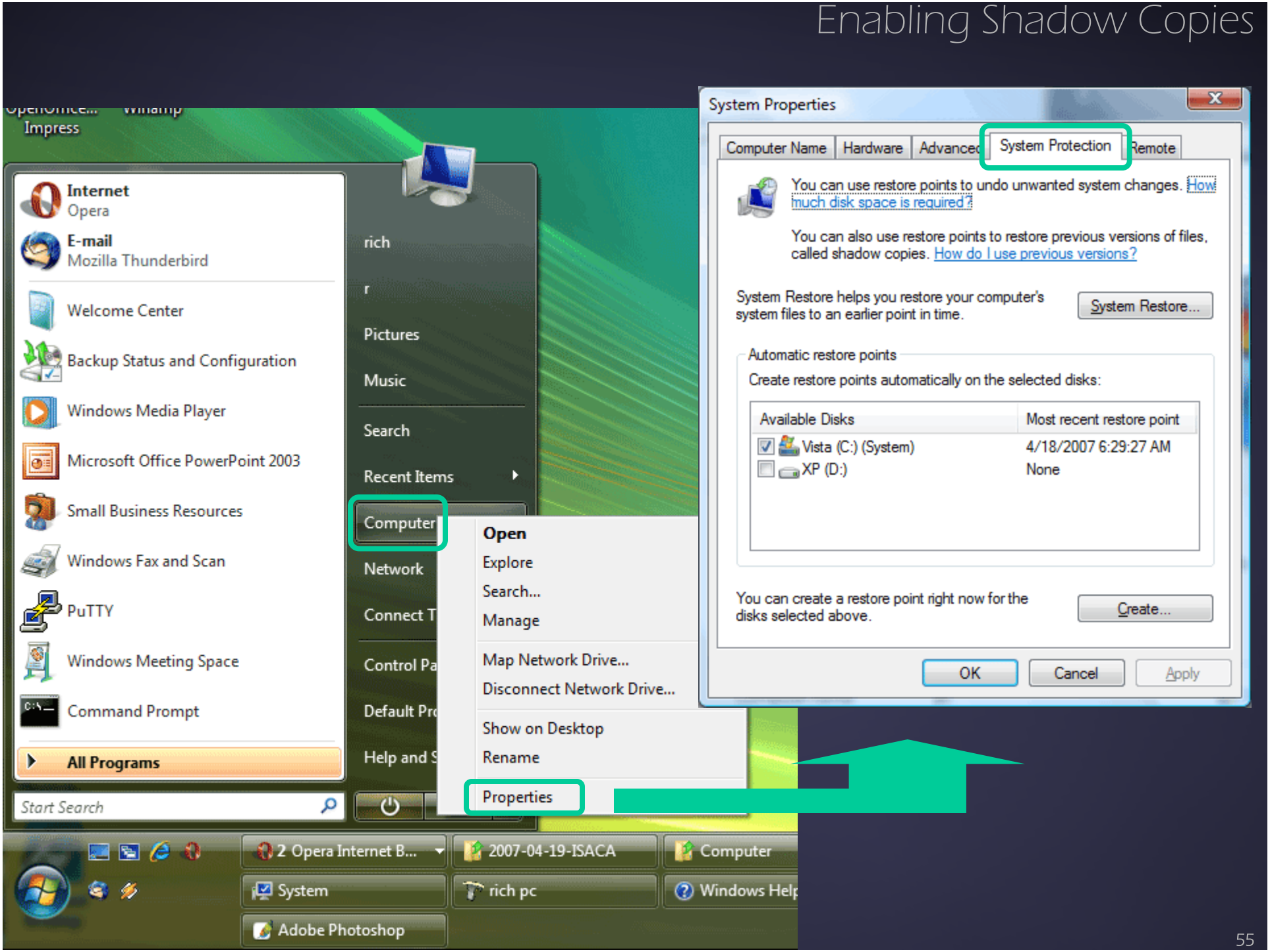
Disk After

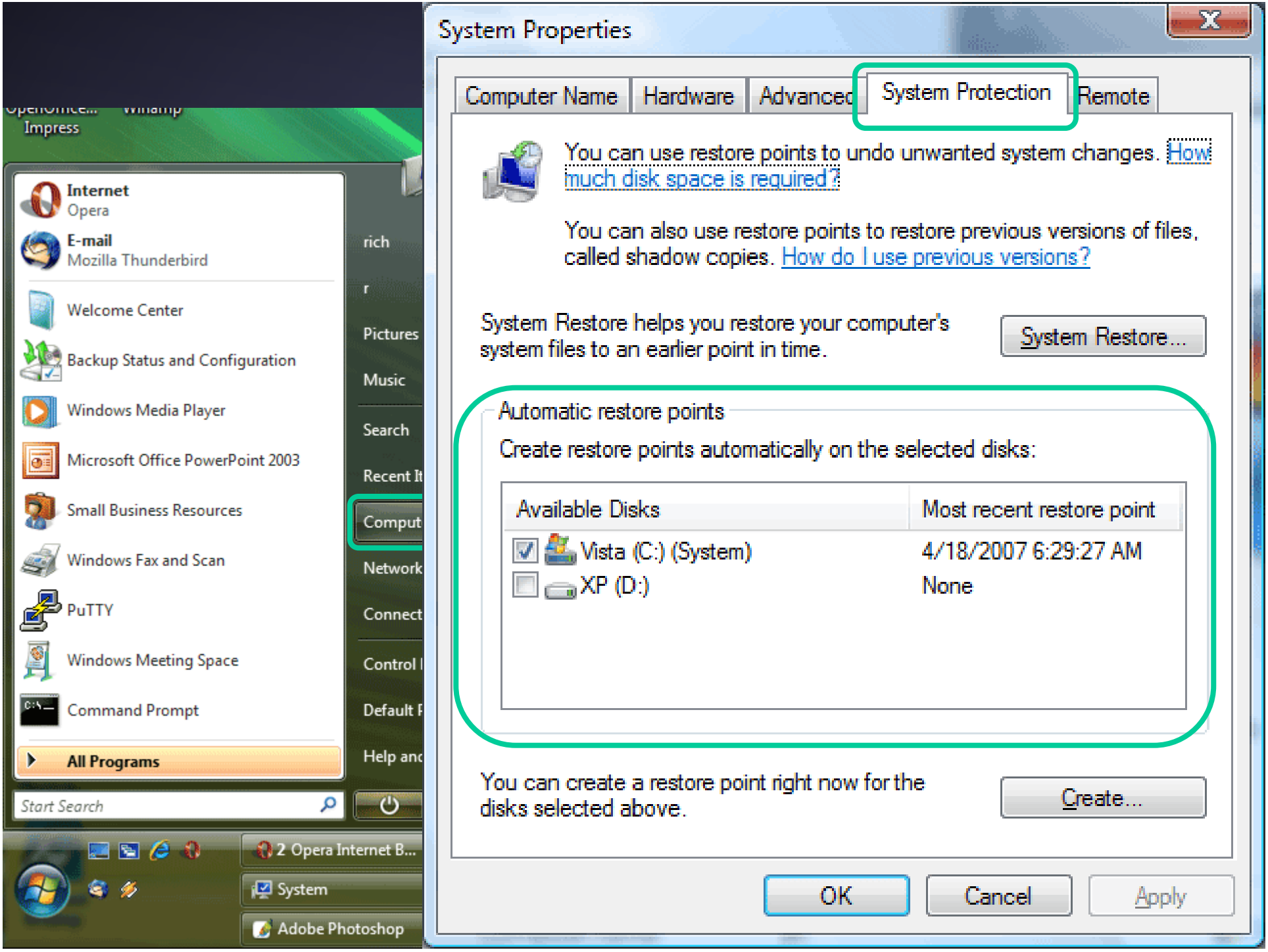
shadow copy holds only blocks that changed.

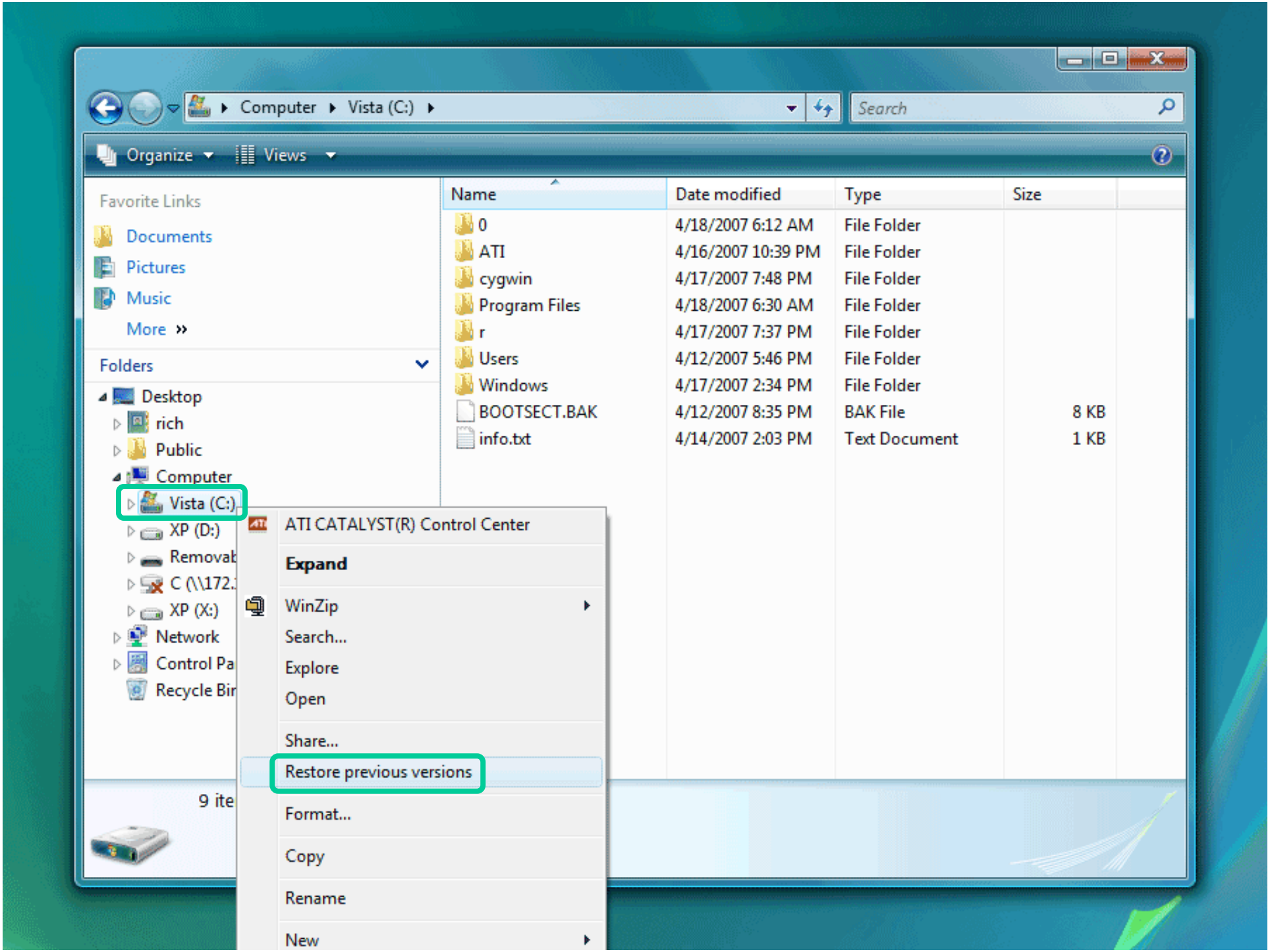


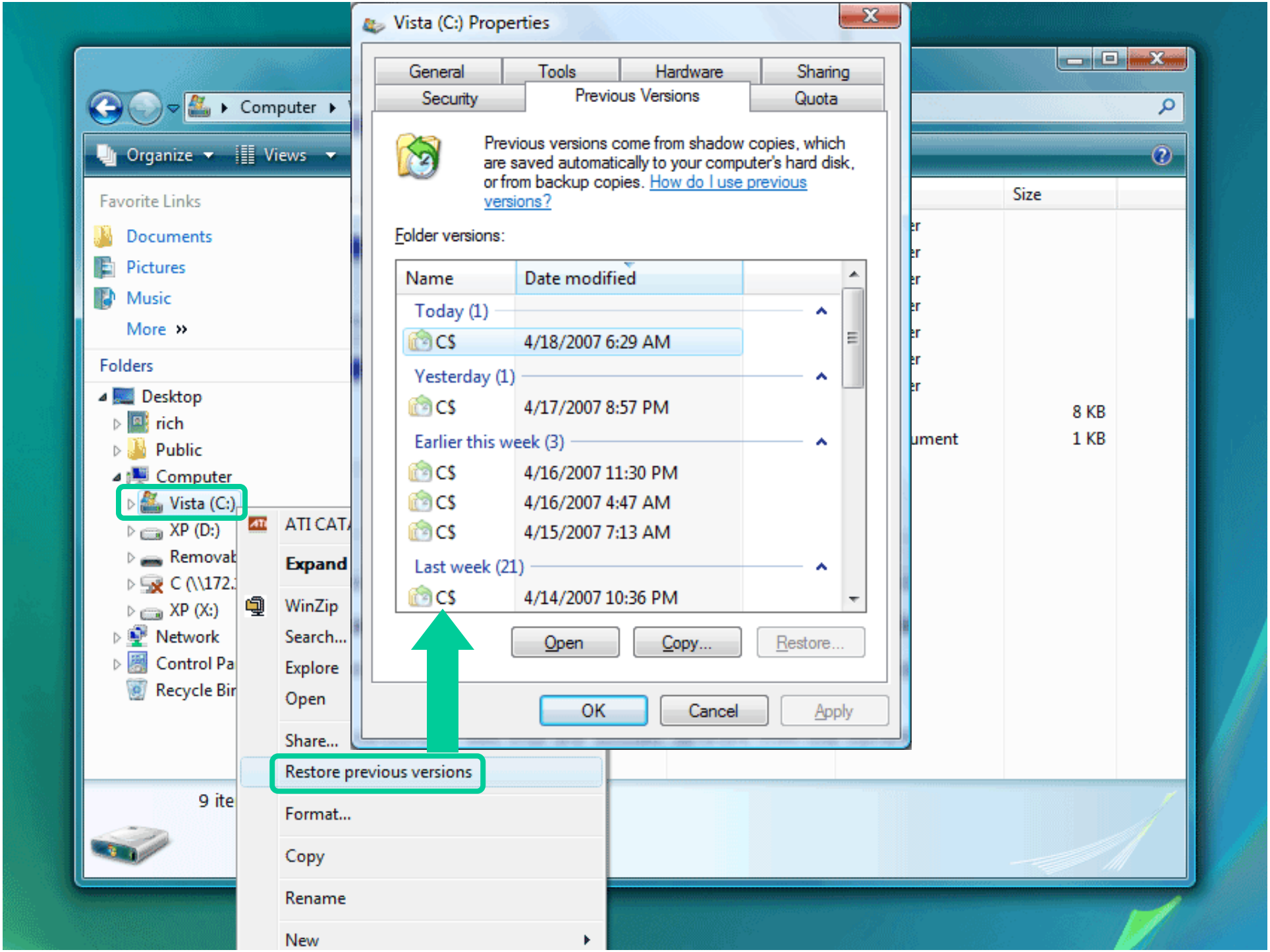
Shadow After

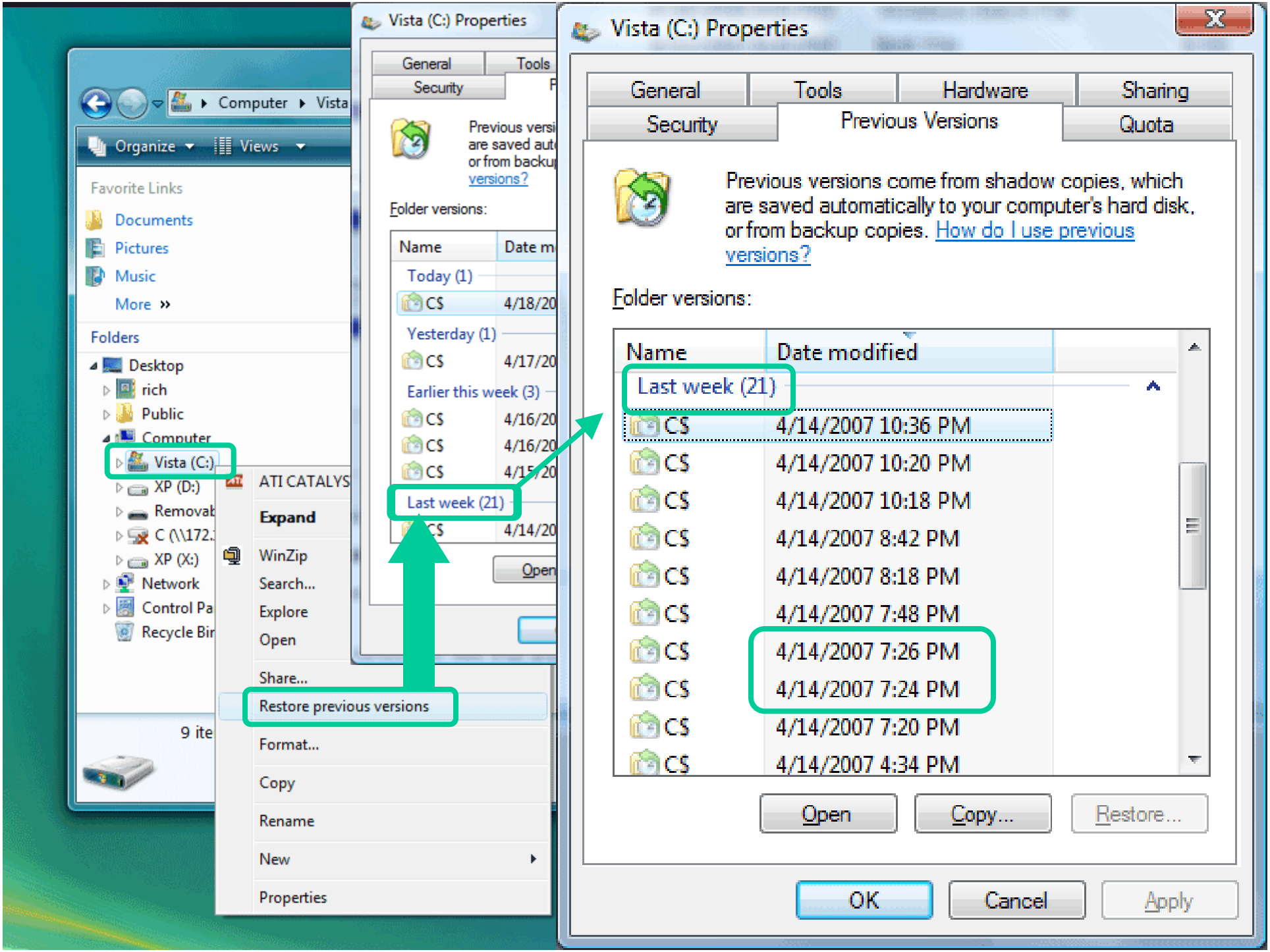
Enabling Shadow Copies

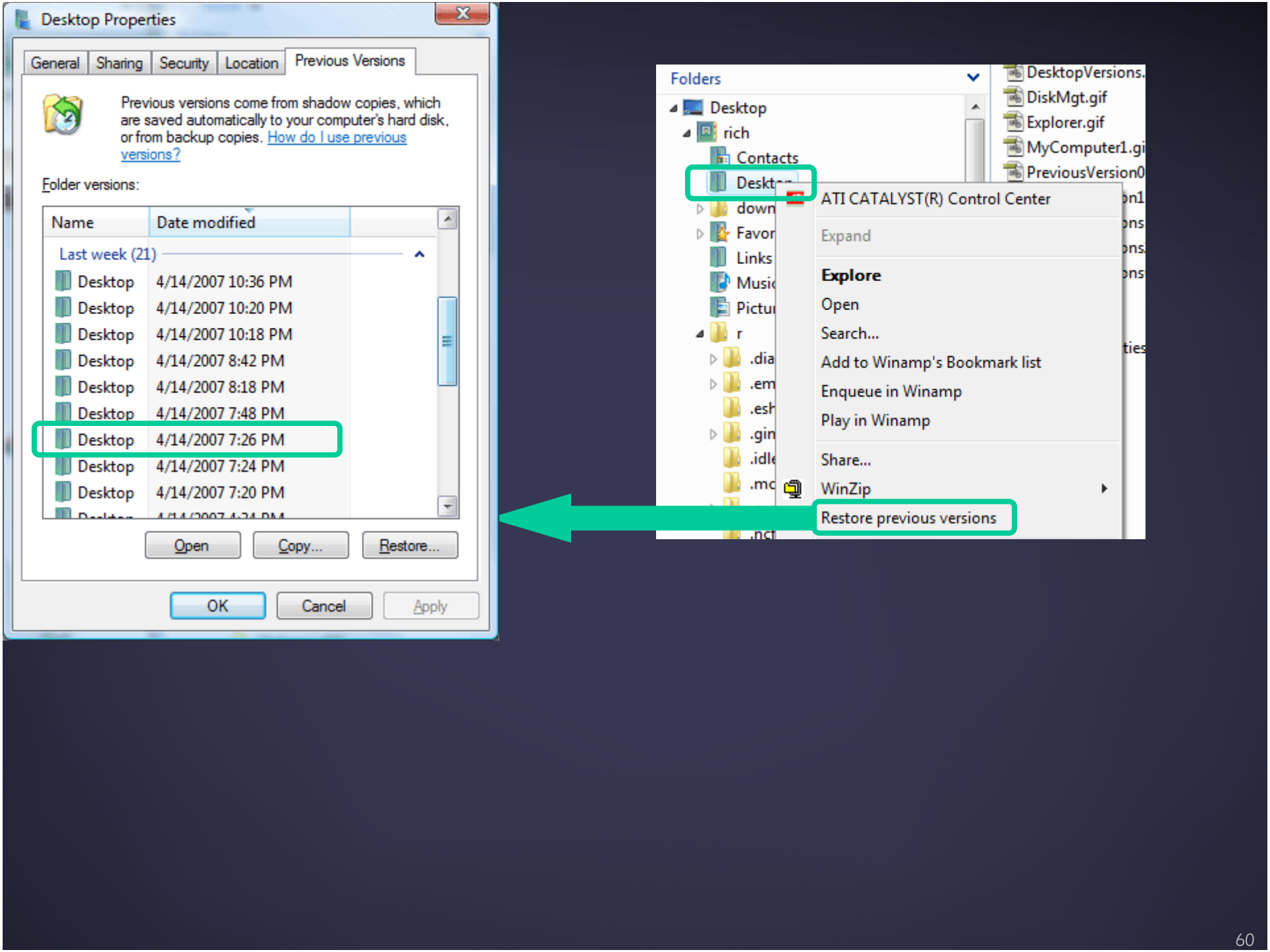


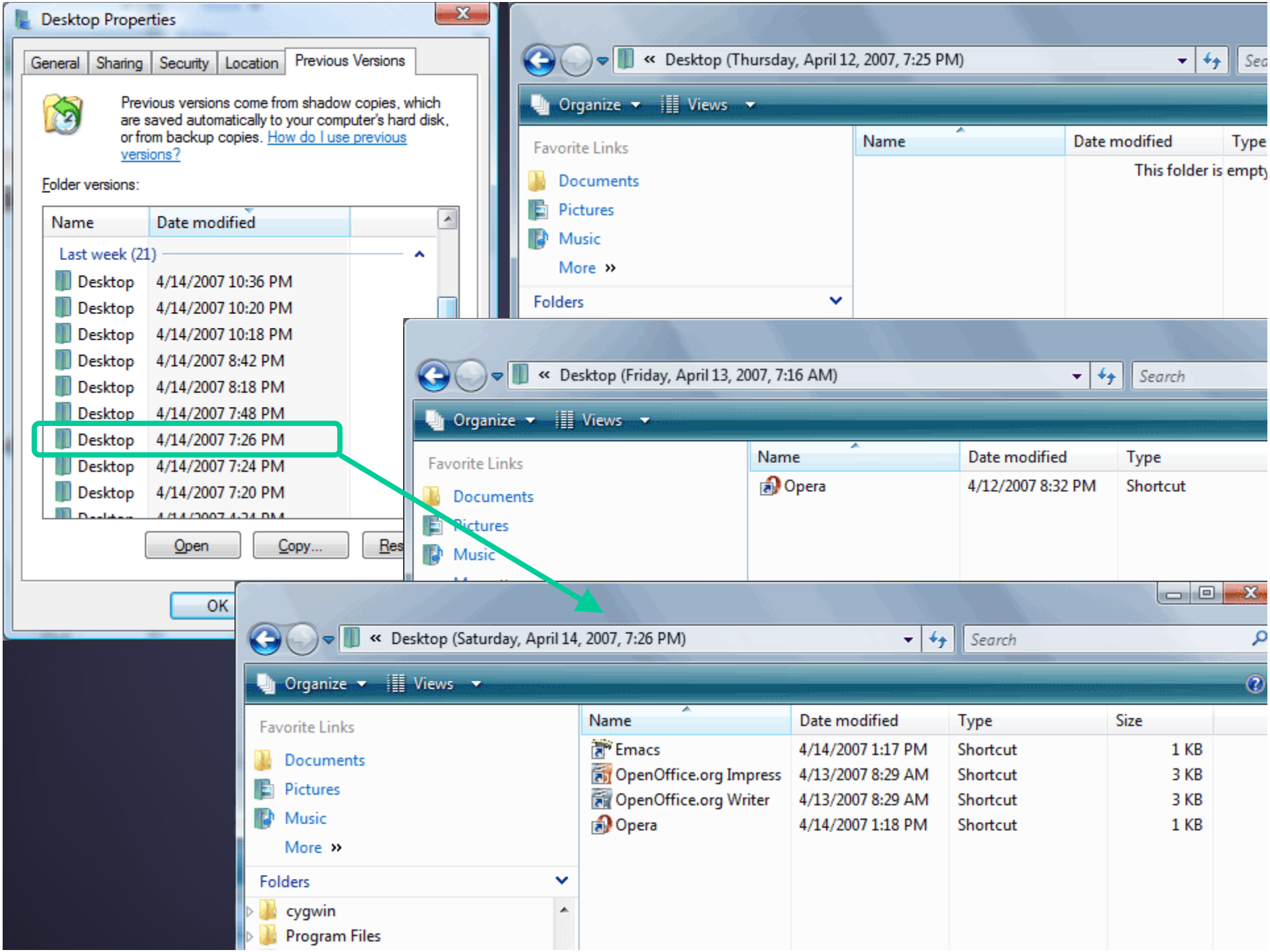

Impress
Internet
Opera
E-mail
Mozilla Thunderbird
Welcome Center
Backup Status and Configuration
Windows Media Player
Microsoft Office PowerPoint 2003
Small Business Resources
Windows Fax and Scan
PuTTY
Windows Meeting Space
Command Prompt
All Programs
Start Search
rich
Pictures
Music
Search
Recent It
Comput
Network
Connect
Control
Default
Help and
2 Opera Internet B...
System
Adobe Photoshop
System Properties
Computer Name
Hardware
Advanced
System Protection
Remote
You can use restore points to undo unwanted system changes. How much disk space is required?
You can also use restore points to restore previous versions of files, called shadow copies. How do I use previous versions?
System Restore helps you restore your computer's system files to an earlier point in time.
System Restore...
Automatic restore points
Create restore points automatically on the selected disks:
Available Disks
Most recent restore point
Vista (C:) (System)
4/18/2007 6:29:27 AM
XP (D:)
None
You can create a restore point right now for the disks selected above.
Create...
OK
Cancel
Apply

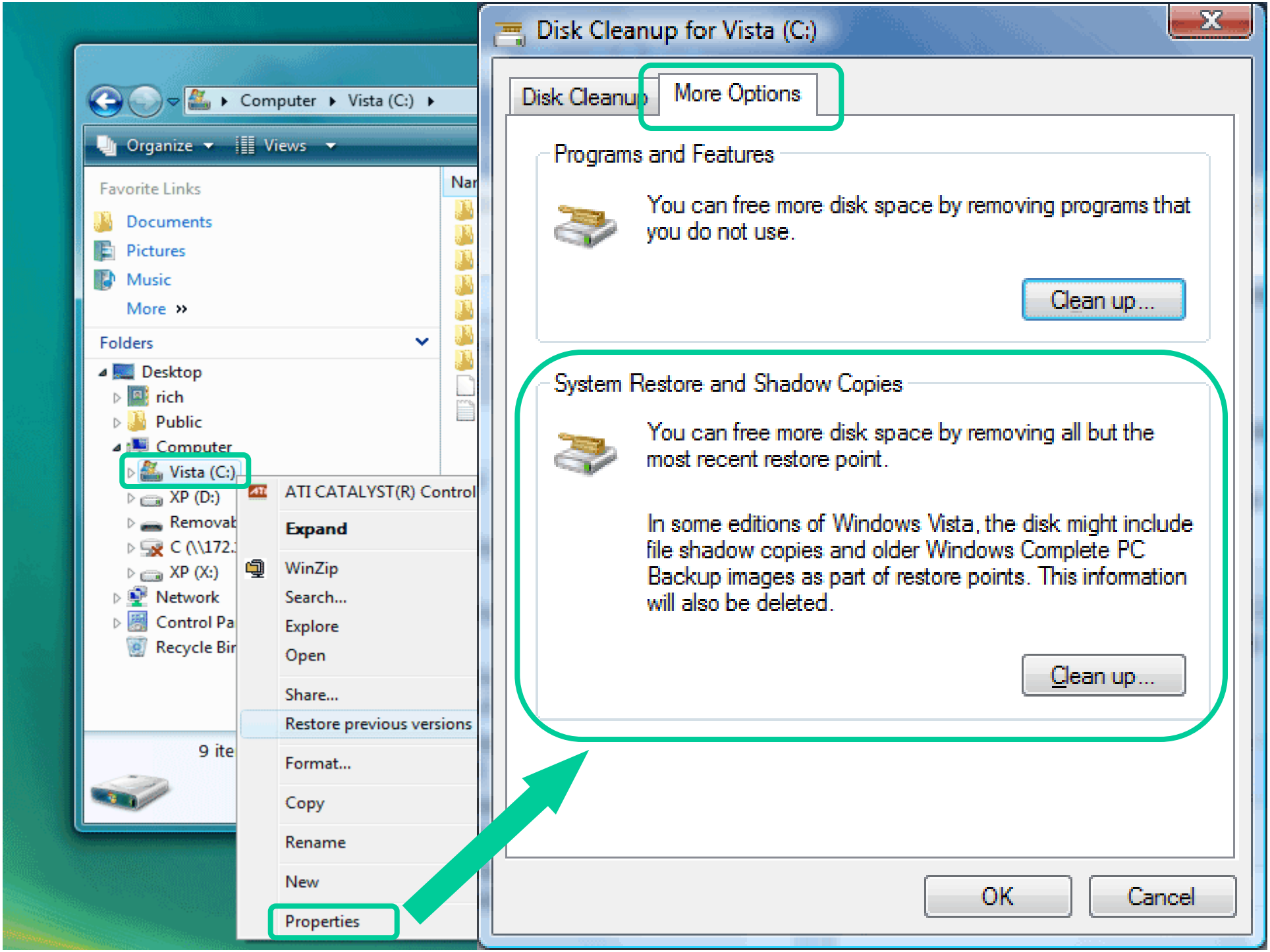

Computer ▸ Vista (C:) ▸
Search
Organize
Views
Favorite Links
Documents
Pictures
Music
More »
Folders
Desktop
rich
Public
Computer
Vista (C:)
XP (D:)
Removab
C (\\172.
XP (X:)
Network
Control Pa
Recycle Bir
Name
Date modified
Type
Size
0 4/18/2007 6:12 AM File Folder
ATI 4/16/2007 10:39 PM File Folder
cygwin 4/17/2007 7:48 PM File Folder
Program Files 4/18/2007 6:30 AM File Folder
r 4/17/2007 7:37 PM File Folder
Users 4/12/2007 5:46 PM File Folder
Windows 4/17/2007 2:34 PM File Folder
BOOTSECT.BAK 4/12/2007 8:35 PM BAK File 8 KB
info.txt 4/14/2007 2:03 PM Text Document 1 KB
9 ite
ATI CATALYST(R) Control Center
Expand
WinZip
Search...
Explore
Open
Share...
Restore previous versions
Format...
Copy
Rename
New

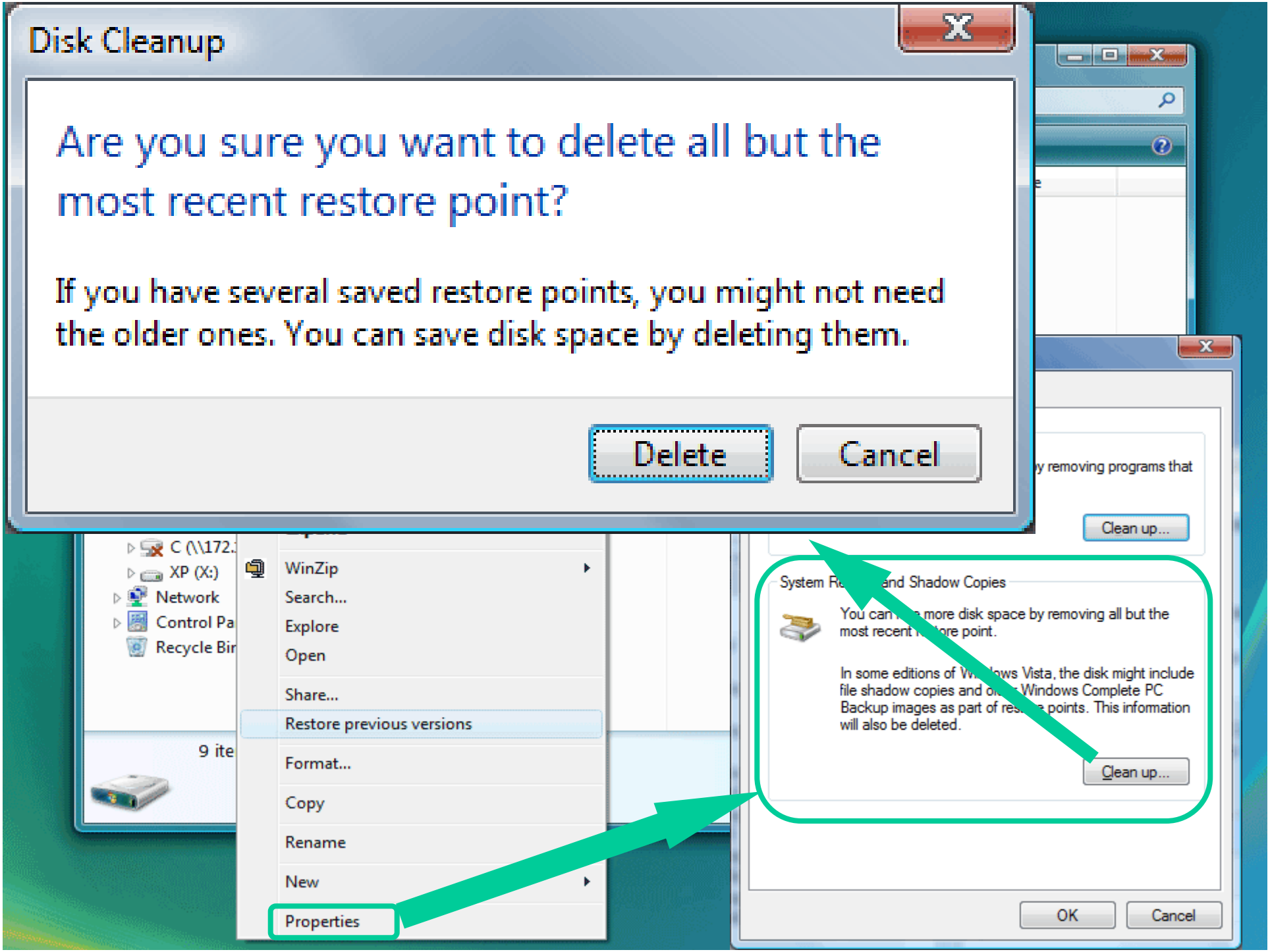

Vista (C:) Properties
General
Tools
Hardware
Sharing
Security
Previous Versions
Quota
Previous versions come from shadow copies, which are saved automatically to your computer's hard disk, or from backup copies. How do I use previous versions?
Folder versions:
Name
Date modified
Today (1)
C$ 4/18/2007 6:29 AM
Yesterday (1)
C$ 4/17/2007 8:57 PM
Earlier this week (3)
C$ 4/16/2007 11:30 PM
C$ 4/16/2007 4:47 AM
C$ 4/15/2007 7:13 AM
Last week (21)
C$ 4/14/2007 10:36 PM
Open
Copy...
Restore...
OK
Cancel
Apply
Computer
Organize
Views
Favorite Links
Documents
Pictures
Music
More
Folders
Desktop
rich
Public
Computer
Vista (C:)
XP (D:)
Network
Control Pa
Recycle Bir
Size
8 KB
1 KB
ATI CAT
Expand
WinZip
Search...
Explore
Open
Share...
Restore previous versions
Format...
Copy
Rename
New

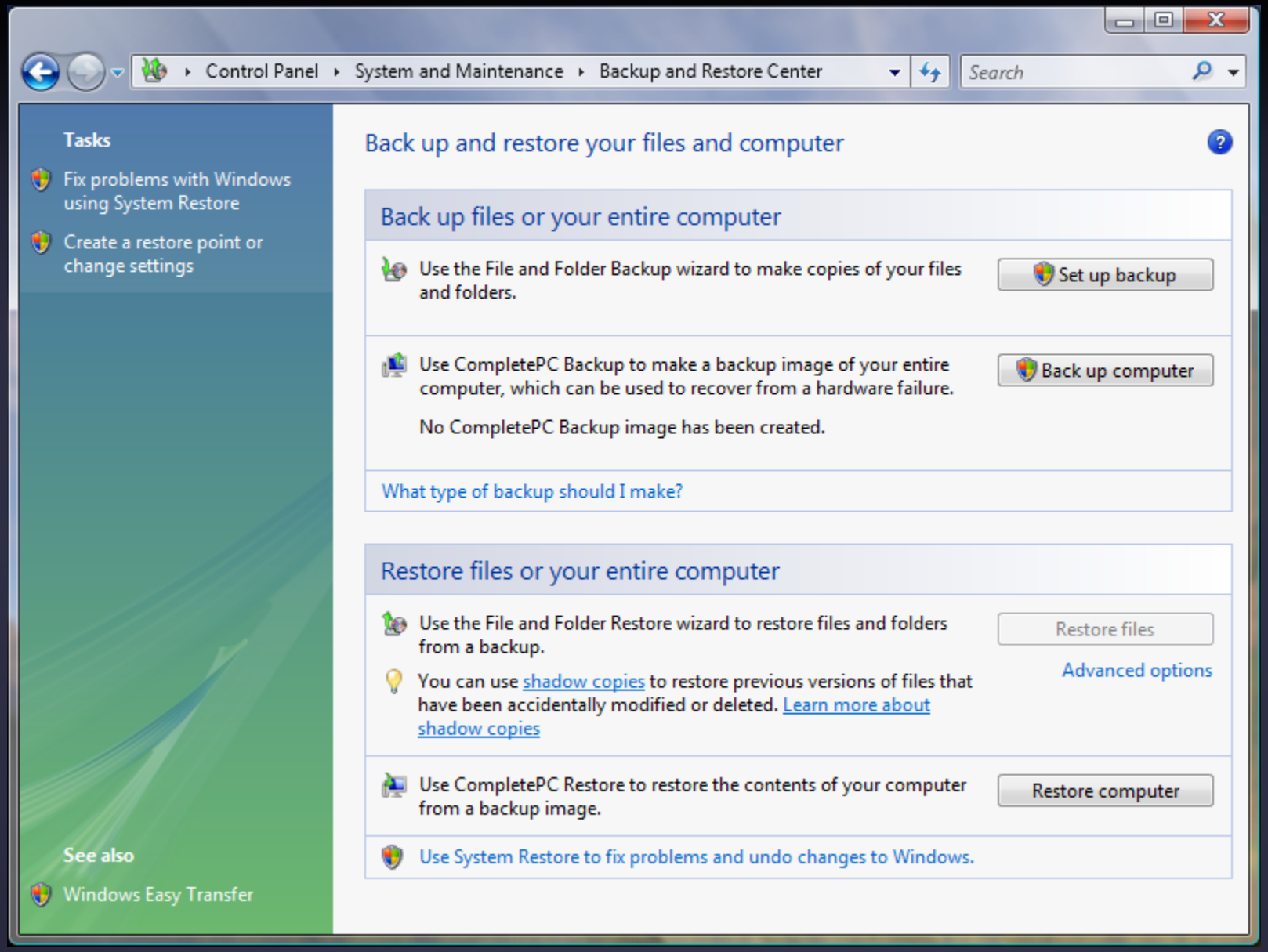

Computer ▸ Vista
Organize
Views
Favorite Links
Documents
Pictures
Music
More »
Folders
Desktop
rich
Public
Computer
Vista (C:)
XP (D:)
XP (X:)
Network
Control Pa
Recycle Bir
9 ite
ATI CATALYS
Expand
WinZip
Search...
Explore
Open
Share...
Restore previous versions
Format...
Copy
Rename
New
Properties
Vista (C:) Properties
General
Tools
Security
Folder versions:
Name
Date m
Today (1)
C$ 4/18/20
Yesterday (1)
C$ 4/17/20
Earlier this week (3)
C$ 4/16/20
C$ 4/16/20
C$ 4/15/20
Last week (21)
C$ 4/14/20
Open
Vista (C:) Properties
General
Tools
Hardware
Sharing
Security
Previous Versions
Quota
Previous versions come from shadow copies, which are saved automatically to your computer's hard disk, or from backup copies. How do I use previous versions?
Folder versions:
Name
Date modified
Last week (21)
C$ 4/14/2007 10:36 PM
C$ 4/14/2007 10:20 PM
C$ 4/14/2007 10:18 PM
C$ 4/14/2007 8:42 PM
C$ 4/14/2007 8:18 PM
C$ 4/14/2007 7:48 PM
C$ 4/14/2007 7:26 PM
C$ 4/14/2007 7:24 PM
C$ 4/14/2007 7:20 PM
C$ 4/14/2007 4:34 PM
Open
Copy...
Restore...
OK
Cancel
Apply

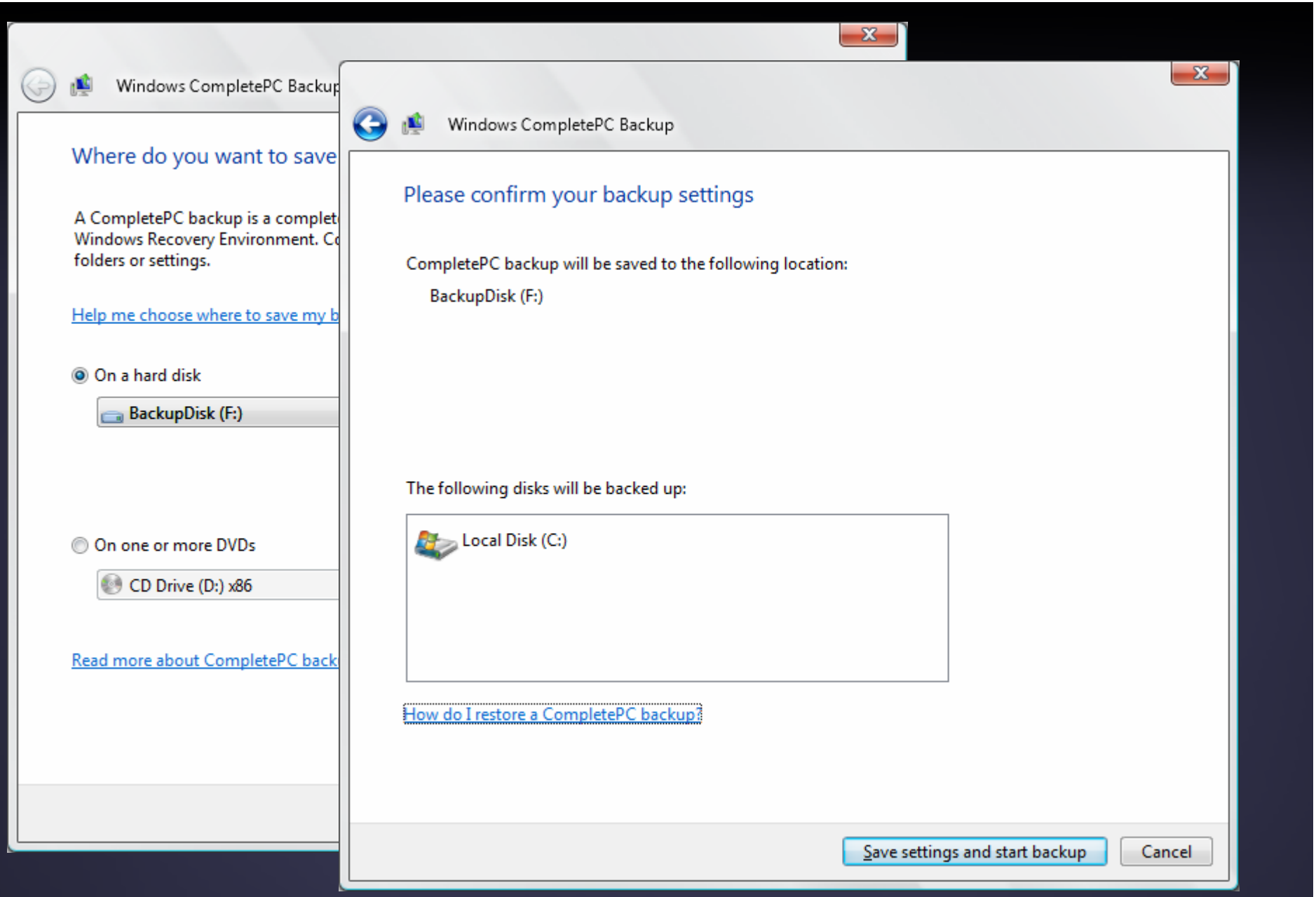

Desktop Properties
General
Sharing
Security
Location
Previous Versions
Previous versions come from shadow copies, which are saved automatically to your computer's hard disk, or from backup copies. How do I use previous versions?
Folder versions:
Name
Date modified
Last week (21)
Desktop 4/14/2007 10:36 PM
Desktop 4/14/2007 10:20 PM
Desktop 4/14/2007 10:18 PM
Desktop 4/14/2007 8:42 PM
Desktop 4/14/2007 8:18 PM
Desktop 4/14/2007 7:48 PM
Desktop 4/14/2007 7:26 PM
Desktop 4/14/2007 7:24 PM
Desktop 4/14/2007 7:20 PM
Open
Copy...
Restore...
OK
Cancel
Apply
Folders
Desktop
rich
Contacts
Links
DesktopVersions.
DiskMgt.gif
Explorer.gif
MyComputer1.gi
PreviousVersion0
ATI CATALYST(R) Control Center
Expand
Explore
Open
Search...
Add to Winamp's Bookmark list
Enqueue in Winamp
Play in Winamp
Share...
WinZip
Restore previous versions


Desktop Properties
General
Sharing
Security
Location
Previous Versions
Previous versions come from shadow copies, which are saved automatically to your computer's hard disk, or from backup copies. How do I use previous versions?
Folder versions:
Name
Date modified
Last week (21)
Desktop 4/14/2007 10:36 PM
Desktop 4/14/2007 10:20 PM
Desktop 4/14/2007 10:18 PM
Desktop 4/14/2007 8:42 PM
Desktop 4/14/2007 8:18 PM
Desktop 4/14/2007 7:48 PM
Desktop 4/14/2007 7:26 PM
Desktop 4/14/2007 7:24 PM
Desktop 4/14/2007 7:20 PM
Open
Copy...
OK
« Desktop (Thursday, April 12, 2007, 7:25 PM)
Organize
Views
Favorite Links
Documents
Pictures
Music
More »
Folders
Name
Date modified
Type
This folder is empty
« Desktop (Friday, April 13, 2007, 7:16 AM)
Search
Opera
4/12/2007 8:32 PM
Shortcut
« Desktop (Saturday, April 14, 2007, 7:26 PM)
Emacs
4/14/2007 1:17 PM
Shortcut
1 KB
OpenOffice.org Impress
4/13/2007 8:29 AM
3 KB
OpenOffice.org Writer
4/13/2007 8:29 AM
3 KB
Opera
4/14/2007 1:18 PM
1 KB
Size
cygwin
Program Files

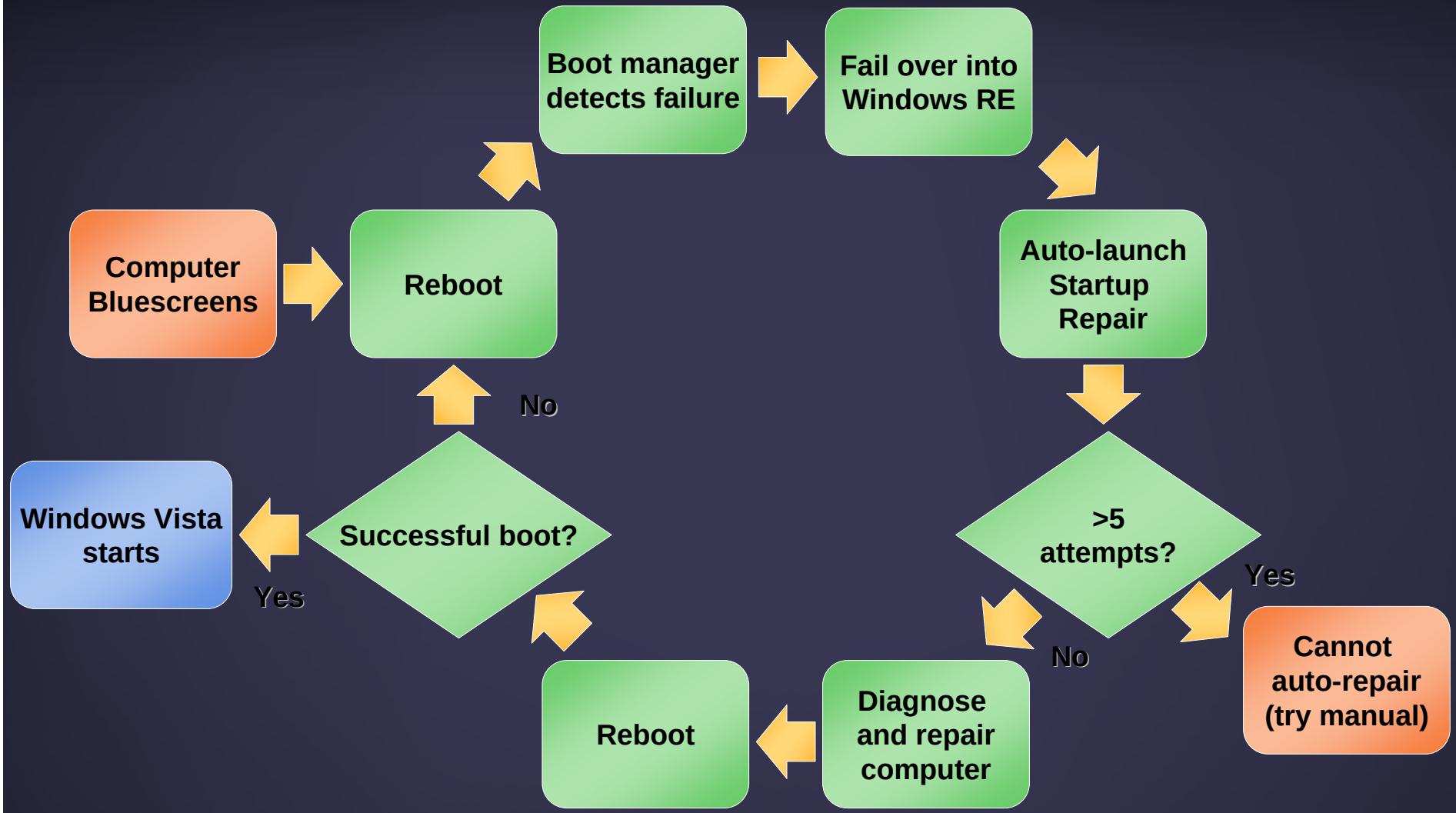

Computer ▸ Vista (C:) ▸
Organize
Views
Favorite Links
Documents
Pictures
Music
More »
Folders
Desktop
rich
Public
Computer
Vista (C:)
XP (D:)
Removab
C (\\172.
XP (X:)
Network
Control Pa
Recycle Bir
9 ite
ATI CATALYST(R) Control
Expand
WinZip
Search...
Explore
Open
Share...
Restore previous versions
Format...
Copy
Rename
New
Properties
Disk Cleanup for Vista (C:)
Disk Cleanup
More Options
Programs and Features
You can free more disk space by removing programs that you do not use.
Clean up...
System Restore and Shadow Copies
You can free more disk space by removing all but the most recent restore point.
In some editions of Windows Vista, the disk might include file shadow copies and older Windows Complete PC Backup images as part of restore points. This information will also be deleted.
Clean up...
OK
Cancel

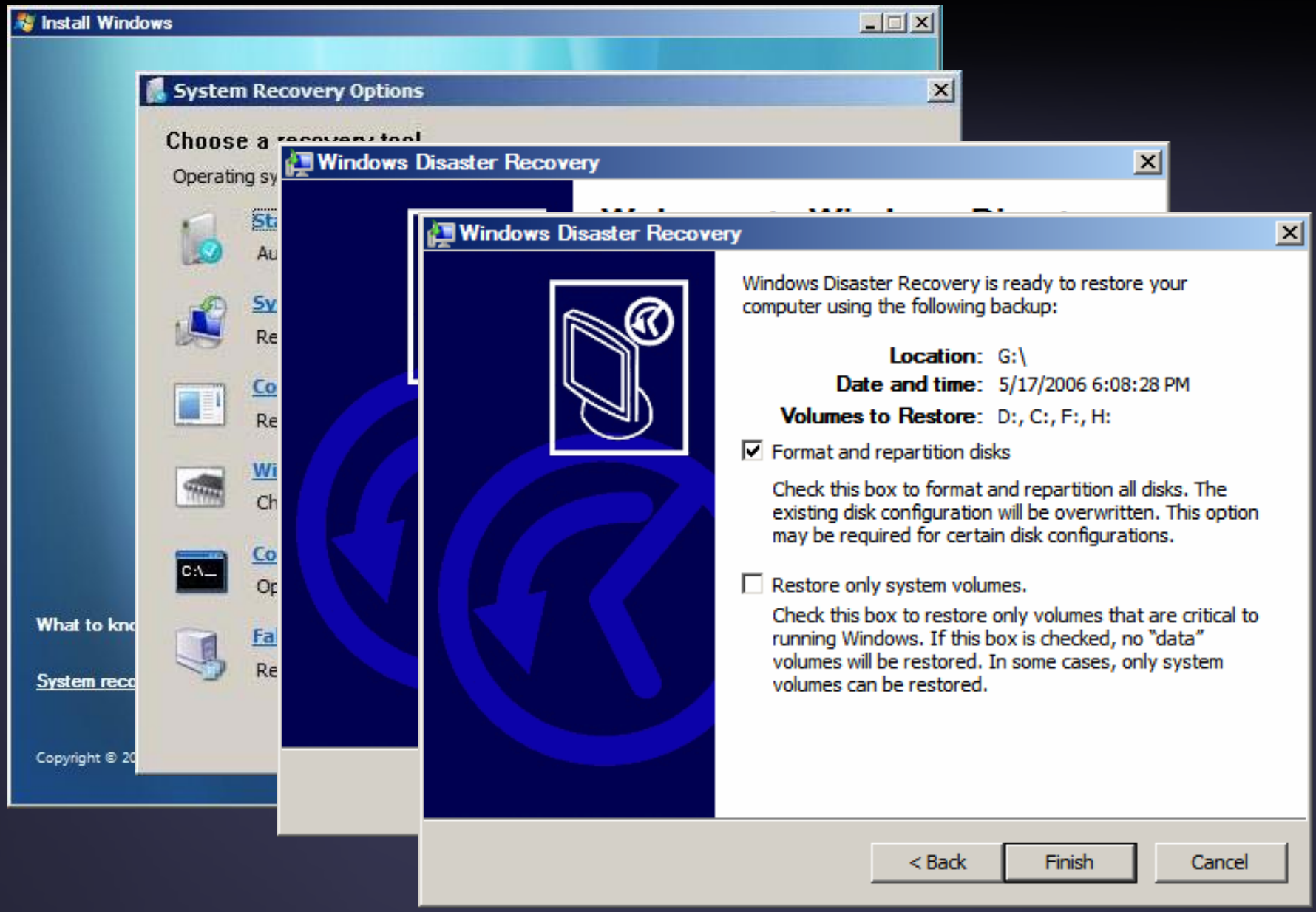

Disk Cleanup
Are you sure you want to delete all but the most recent restore point?
If you have several saved restore points, you might not need the older ones. You can save disk space by deleting them.
Delete
Cancel
WinZip
Search...
Explore
Open
Share...
Restore previous versions
Format...
Copy
Rename
New
Properties
Network
Recycle Bin
removing programs that
Clean up...
and Shadow Copies
more disk space by removing all but the most recent restore point.
In some editions of Windows Vista, the disk might include file shadow copies and other Windows Complete PC Backup images as part of restore points. This information will also be deleted.
Clean up...
OK
Cancel


Control Panel ▸ System and Maintenance ▸ Backup and Restore Center
Search
Tasks
Fix problems with Windows using System Restore
Create a restore point or change settings
See also
Windows Easy Transfer
Back up and restore your files and computer
Back up files or your entire computer
Use the File and Folder Backup wizard to make copies of your files and folders.
Set up backup
Use CompletePC Backup to make a backup image of your entire computer, which can be used to recover from a hardware failure.
No CompletePC Backup image has been created.
Back up computer
What type of backup should I make?
Restore files or your entire computer
Use the File and Folder Restore wizard to restore files and folders from a backup.
Restore files
Advanced options
You can use shadow copies to restore previous versions of files that have been accidentally modified or deleted. Learn more about shadow copies
Use CompletePC Restore to restore the contents of your computer from a backup image.
Restore computer
Use System Restore to fix problems and undo changes to Windows.


Windows CompletePC Backup
Where do you want to save
A CompletePC backup is a complet
Windows Recovery Environment. C
folders or settings.
Help me choose where to save my b
On a hard disk
BackupDisk (F:)
On one or more DVDs
CD Drive (D:) x86
Read more about CompletePC back
Windows CompletePC Backup
Please confirm your backup settings
CompletePC backup will be saved to the following location:
BackupDisk (F:)
The following disks will be backed up:
Local Disk (C:)
How do I restore a CompletePC backup?
Save settings and start backup
Cancel

Windows RE Auto-Repair




Install Windows
System Recovery Options
Choose a
Operating sy
What to kn
System reco
Copyright © 20
Windows Disaster Recovery
Windows Disaster Recovery
Windows Disaster Recovery is ready to restore your computer using the following backup:
Location: G:\
Date and time: 5/17/2006 6:08:28 PM
Volumes to Restore: D:, C:, F:, H:
Format and repartition disks
Check this box to format and repartition all disks. The existing disk configuration will be overwritten. This option may be required for certain disk configurations.
Restore only system volumes.
Check this box to restore only volumes that are critical to running Windows. If this box is checked, no "data" volumes will be restored. In some cases, only system volumes can be restored.
< Back
Finish
Cancel

```
C:\>vssadmin /?
vssadmin 1.1 - Volume Shadow Copy Service administrative command-
      line tool
(C) Copyright 2001 Microsoft Corp.

---- Commands Supported ----

Add ShadowStorage     - Add a new volume shadow copy storage
      association
Create Shadow         - Create a new volume shadow copy
Delete Shadows        - Delete volume shadow copies
Delete ShadowStorage  - Delete volume shadow copy storage associations
List Providers        - List registered volume shadow copy providers
List Shadows          - List existing volume shadow copies
List ShadowStorage    - List volume shadow copy storage associations
List Volumes          - List volumes eligible for shadow copies
List Writers          - List subscribed volume shadow copy writers
Resize ShadowStorage  - Resize a volume shadow copy storage
      association
```

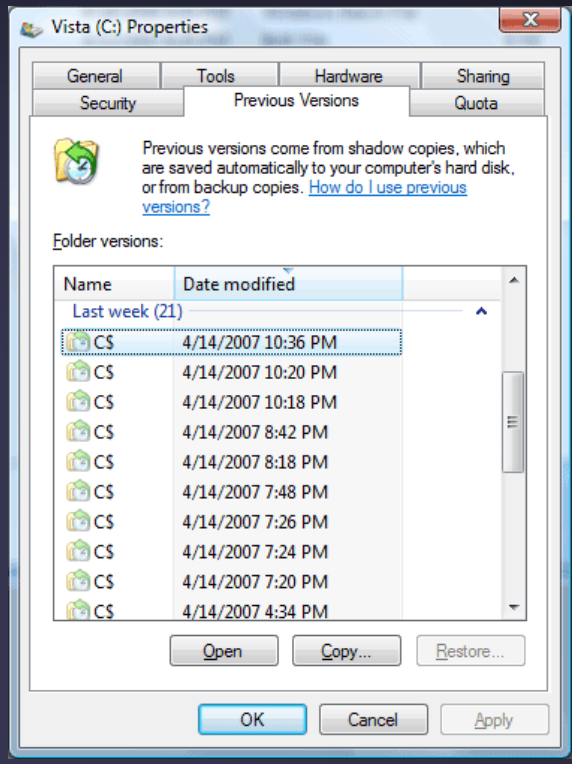
Resource Kit – VolRest

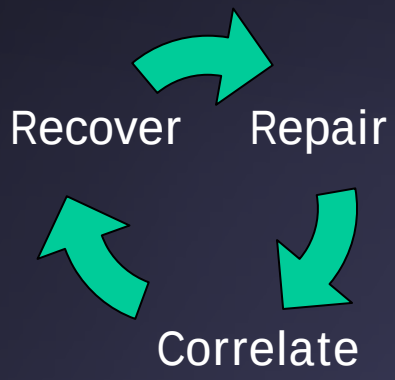
```
C:\Resource Kit>volrest
VOLREST 1.1 - Timewarp Previous Version command-line tool
(C) Copyright 2003 Microsoft Corp.

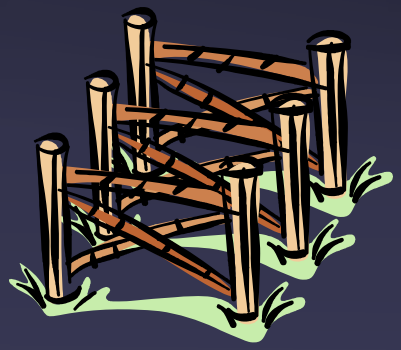
Usage: VOLREST [options] FileName

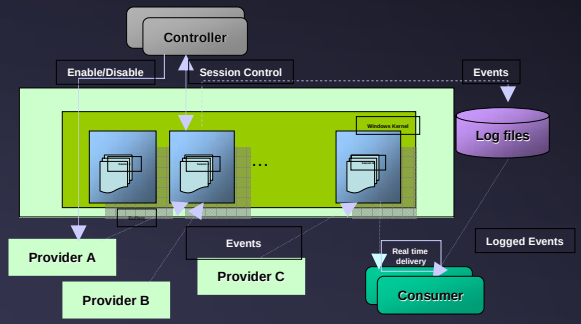
Options are:
   /?    - Displays this help.
   /A    - Includes files with specified attributes.
           /AD  Directories (only).
           /AS  System files.
           /AH  Hidden files.
   /B    - Uses bare format (no heading information or summary).
   /S    - Includes files in specified directory and all subdirectories.
   /R:<DirectoryName> -
           Restore all previous versions in target directory.
   /E    - Restores empty directories (use with /R).
   /SCT  - Decorates restored file names with the shadow copy timestamp.
           Use with /R. For example:
           "foo (Wednesday, January 01, 2003, 14.00.00).doc"

Examples:
   VOLREST Z:\MYDIRECTORY\MYFILE.DOC
   VOLREST //server\share\MYDIRECTORY\*.DOC
   VOLREST Z:\*.* /s /r:C:\OLDFILES
   VOLREST Z:\*.DOC /s /r:C:\OLDFILES /SCT
```









Questions?

Rich@Murphey.org
http://murphey.org
http://acsworldwide.com



- C. R. Murphey, “Automated Windows Event Log Forensics,” Digital Investigation, August 2007

- Digital Forensic Research Workshop, 8/13/07
- GMU Forensics Symposium
- HTCIA National 8/27/07

