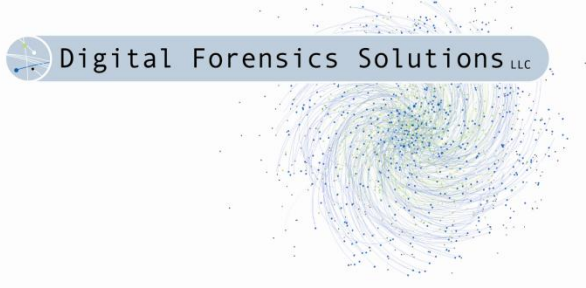


Advanced Registry Forensics with Registry Decoder

Dr. Vico Marziale

Sleuth Kit and Open Source Digital Forensics Conference 2012

10/03/2012

Who am I?

- Senior Security Researcher @ DFS
- Published Researcher
  - DFRWS, IFIP, Journal of Digital Investigation, Research Advances in Digital Forensics, …
- Practitioner
  - Forensic investigations, penetration tests, training
- Developer
  - Co-developer of Scalpel and <surprise> Registry Decoder
- Occasional computer science professor @ UNO

What you already know:

- Why is the registry interesting?
  - Forensics and incident response goldmine
  - Contains time stamped logs of a wealth of user and system activity
- What kind of activity?
  - Removable device activity
    - Including serial number and model name
    - See stuxnet
  - Typed Internet Explorer URLs
  - And …

And More …

- What kind of activity (cont.)?
  - Recently accessed files (per-file-type)
  - Networking information
    - Device,
    - Network shares, and
    - Routing info …
  - Entered search terms (Windows 7)
  - Autoruns
  - Timezone info
  - Application launch counts
  - And …

And More …

- What kind of activity (cont.)?
  - Mounted devices
  - Installed services
  - System install info
  - Folder listings
  - Firewall rules
  - More discovered all the time …
    - Windows 8 password hints
    - Editing-enabled downloaded Office files

Where is the stuff?

- Sure, the currently active registry files
- And Windows automated backups
  - System Restore
  - VSS
  - We can recover historical data going back months or longer (how?)
  - Recent (normal) case > 60 System Restore Points
- Per machine …
- What do you use to analyze all these?

Good Question?

- Regedit
  - F3 crappy search, no plugins, no lastwrite, live files only, try to copy a path, then shoot self, no reporting
- Regripper
  - Great set of plugins, no GUI browsing, no search
- Access Data Registry Viewer
  - GUI and some search, single file, no plugins
- FTK, Encase
  - GUI, indexed search (no context), plugins?? …
  - … as far as I know; I'm not paying for them
- Why is this so difficult?

Registry Decoder

- Open source Python project
- Initially funded by NIJ
- With some current support from NIST
- Its goal is to help automate the acquisition, analysis, and reporting of registry contents
- Contains two components:
  - A live acquisition tool (Registry Decoder Live)
  - An offline analysis tool (Registry Decoder)
- Recently nominated for Forensic 4cast award for "Best Computer Forensic Software"

Registry Decoder Live

- Performs live acquisition of hive files
- Supports XP, Vista, and 7, 32/64 bit
- Can acquire historical files from the System Restore and Volume Shadow Service
- Creates db that can be imported by RD offline
- Distributed as stand-alone (pyinstaller) exe with no installation requirements / dependencies
  - To ease use/minimize footprint on live machine

Live Acquisition Process

- All current hives and XP backups (System Restore)
  - Using the Sleuth Kit (via pytsk) to read under NTFS
    - Gets around file locking issues
    - Does require admin privileges
  - From C:\Windows\System32\config for current
  - From C:\System Volume Information for backups
- Vista and 7 backups (VSS)
  - For each shadow, create a *SymbolicLink*
  - Simply copy registry files from each

Registry Decoder (Offline)

- Performs offline analysis of registry files
- Facilitates comprehensive registry analysis of any (reasonable) number of files within one graphical interface
  - Interface generates a new tab or tabs for results of each action taken by the user
  - Some features are usable on the command line as well (for scripting, testing, etc.)
    - Soon, all will be (thanks, NIST)

Supported Input Types

- Databases from the live tool
- Individual (or groups of) registry files
- Raw *dd* disk images
- Split *dd* images
- Encase (E01) disk images (not the newest version)
- Encase split images
- Mostly based on Sleuth Kit support
  - Again, via *pytsk*

Processing Individual Files

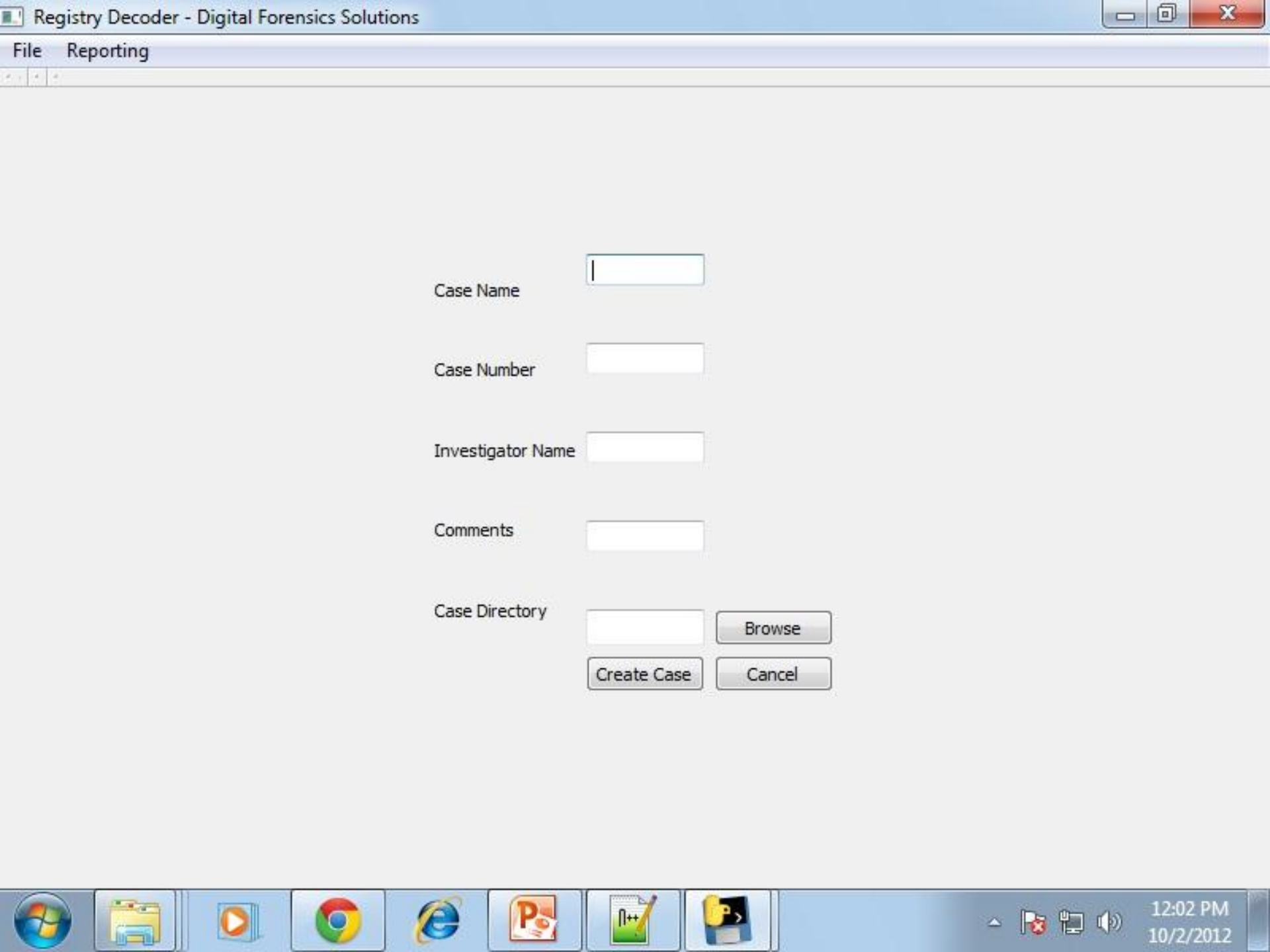
- For individual hives we use the *RegLookup*
  - via *pylibregfi*
- Walk each file and store all key and value (name, type, data) information in SQLite databases and in-memory data structures
  - Can be a bit RAM abusive
- Also use SQLite for string indexing
- Once pre-processing is finished, we no longer need or use the individual registry files

Analysis Features

- Case management
- Hive Browsing
- Advanced Search
- Plugin System
- Path-Based Analysis
- Differencing
- Timelining
- Reporting

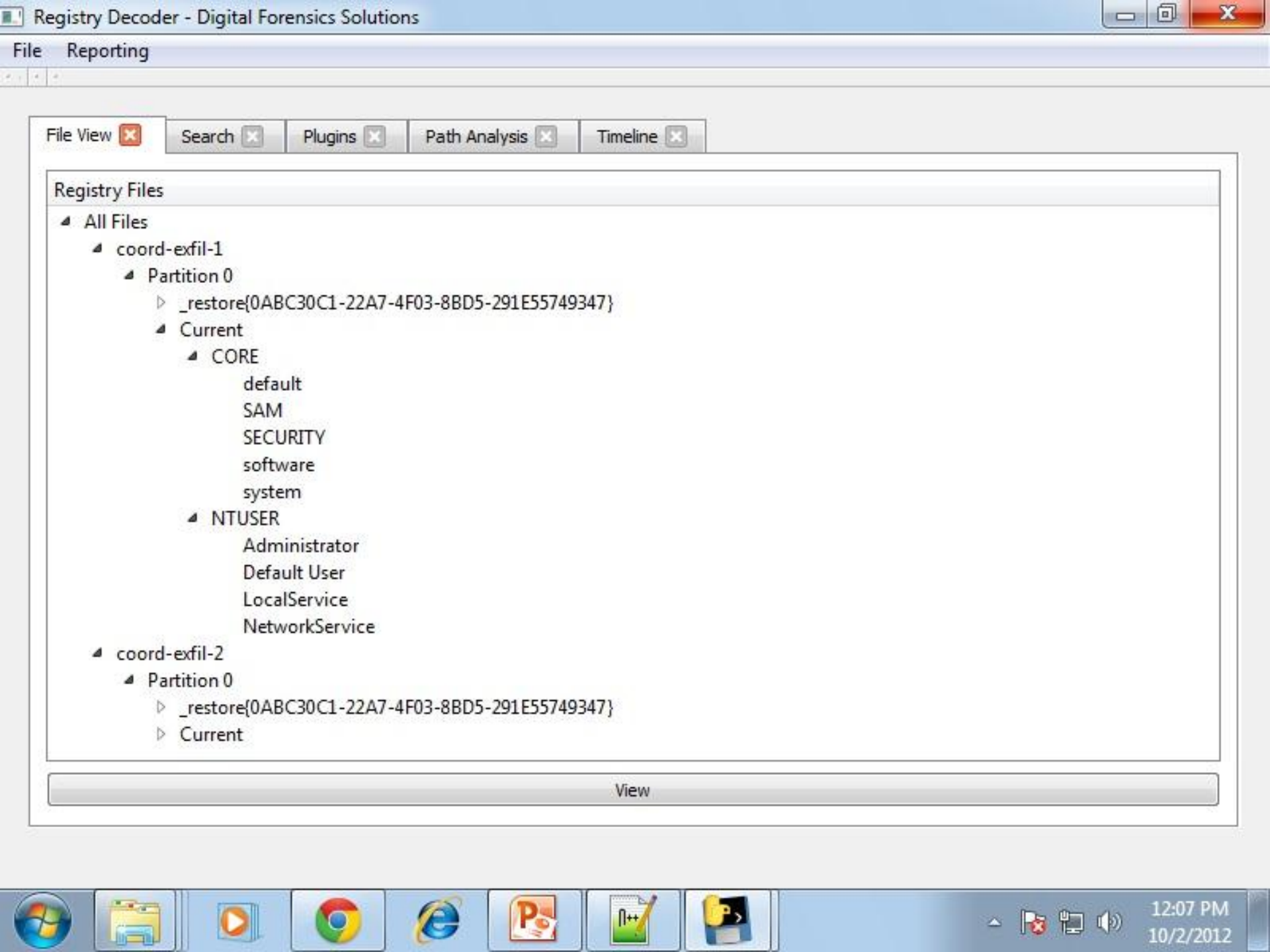
Case Management

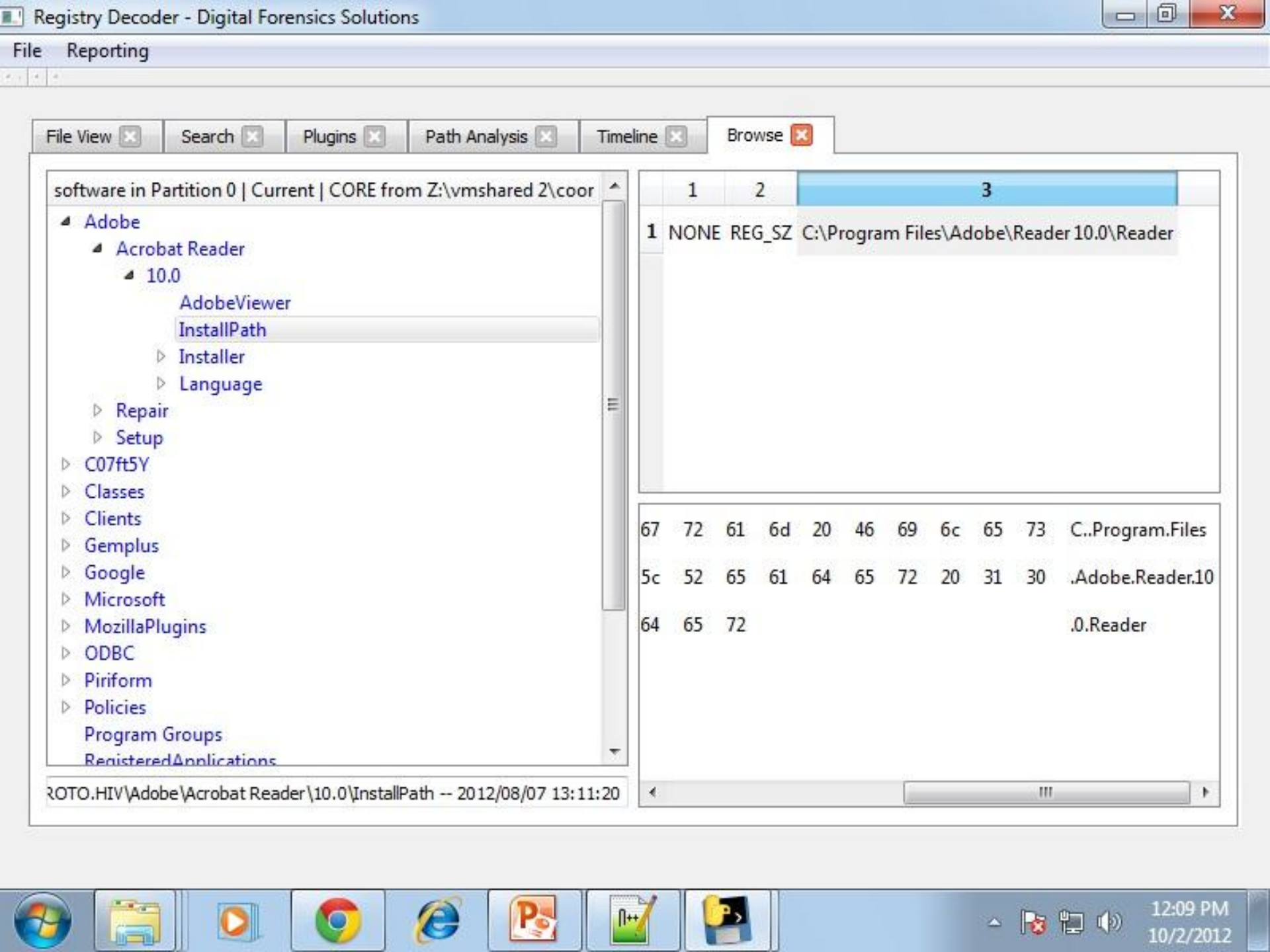
- Simple, but useful
  - Case name, number
  - Investigator
  - Comments
  - Case directory
- Shows up in reports
- Provides persistence
  - Data is only pre-processed once
  - Close and re-open case at will


Registry Decoder - Digital Forensics Solutions
File
Reporting
Case Name
Case Number
Investigator Name
Comments
Case Directory
Browse
Create Case
Cancel
12:02 PM
10/2/2012

Hive Browsing

- Similar to other browsing tools (AccessData, Regedit, etc.) except hierarchical display based on machine/partition/current or backup
- Displays key/value pairs and last write time
- Hex view of value data
- Tabbed view allows multiple browse windows open simultaneously
- Can copy text from most anywhere
- Can type path and immediately jump there


Registry Decoder - Digital Forensics Solutions
File
Reporting
File View
Search
Plugins
Path Analysis
Timeline
Registry Files
All Files
coord-exfil-1
Partition 0
_restore{0ABC30C1-22A7-4F03-8BD5-291E55749347}
Current
CORE
default
SAM
SECURITY
software
system
NTUSER
Administrator
Default User
LocalService
NetworkService
coord-exfil-2
Partition 0
_restore{0ABC30C1-22A7-4F03-8BD5-291E55749347}
Current
View
12:07 PM
10/2/2012

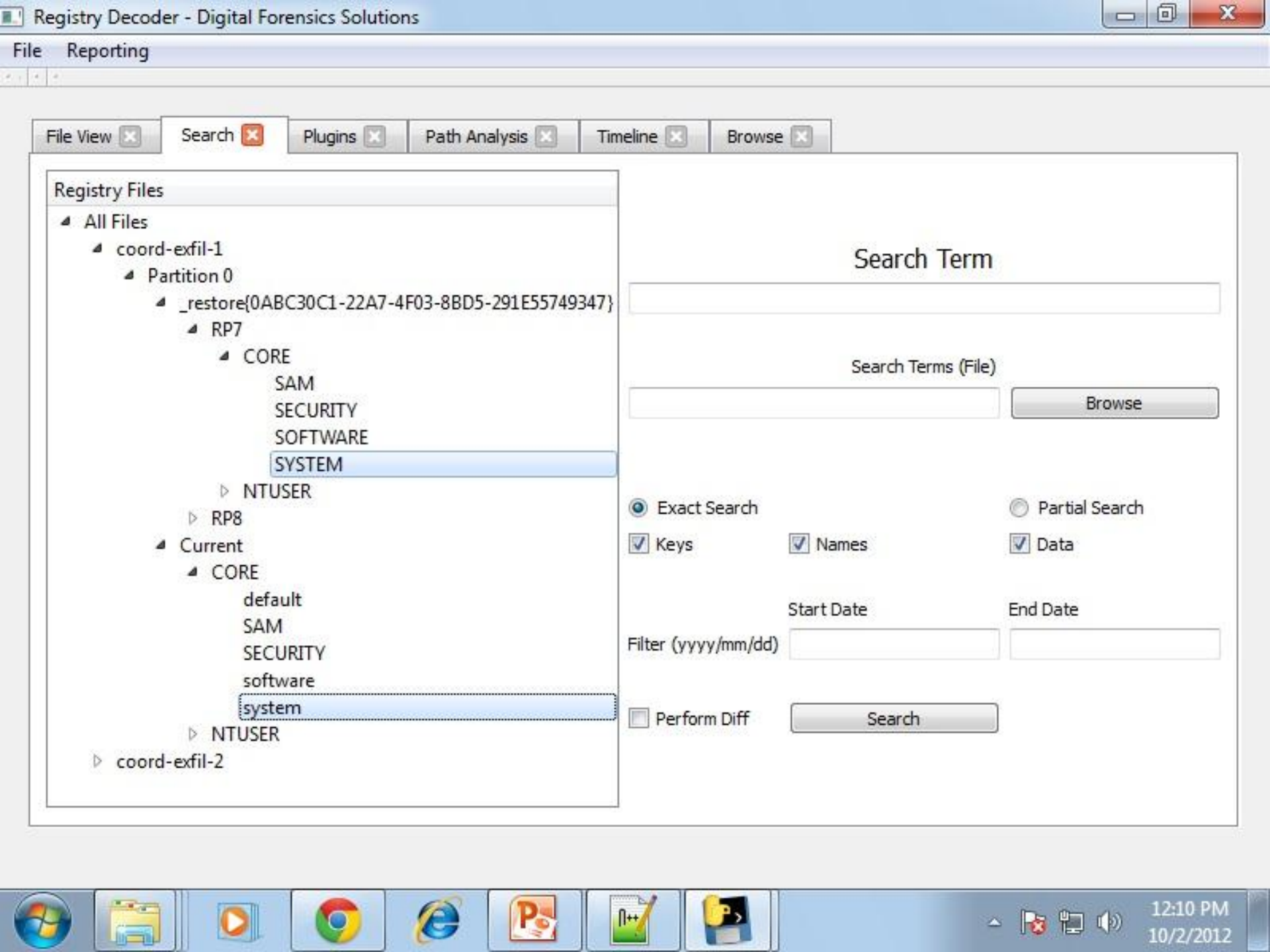

Registry Decoder - Digital Forensics Solutions
File
Reporting
File View
Search
Plugins
Path Analysis
Timeline
Browse
software in Partition 0 | Current | CORE from Z:\vmshared 2\coor
Adobe
Acrobat Reader
10.0
AdobeViewer
InstallPath
Installer
Language
Repair
Setup
C07ft5Y
Classes
Clients
Gemplus
Google
Microsoft
MozillaPlugins
ODBC
Piriform
Policies
Program Groups
RegisteredApplications
ROTO.HIV\Adobe\Acrobat Reader\10.0\InstallPath -- 2012/08/07 13:11:20
1
2
3
1 NONE REG_SZ C:\Program Files\Adobe\Reader 10.0\Reader
67 72 61 6d 20 46 69 6c 65 73 C..Program.Files
5c 52 65 61 64 65 72 20 31 30 .Adobe.Reader.10
64 65 72 .0.Reader
12:09 PM
10/2/2012

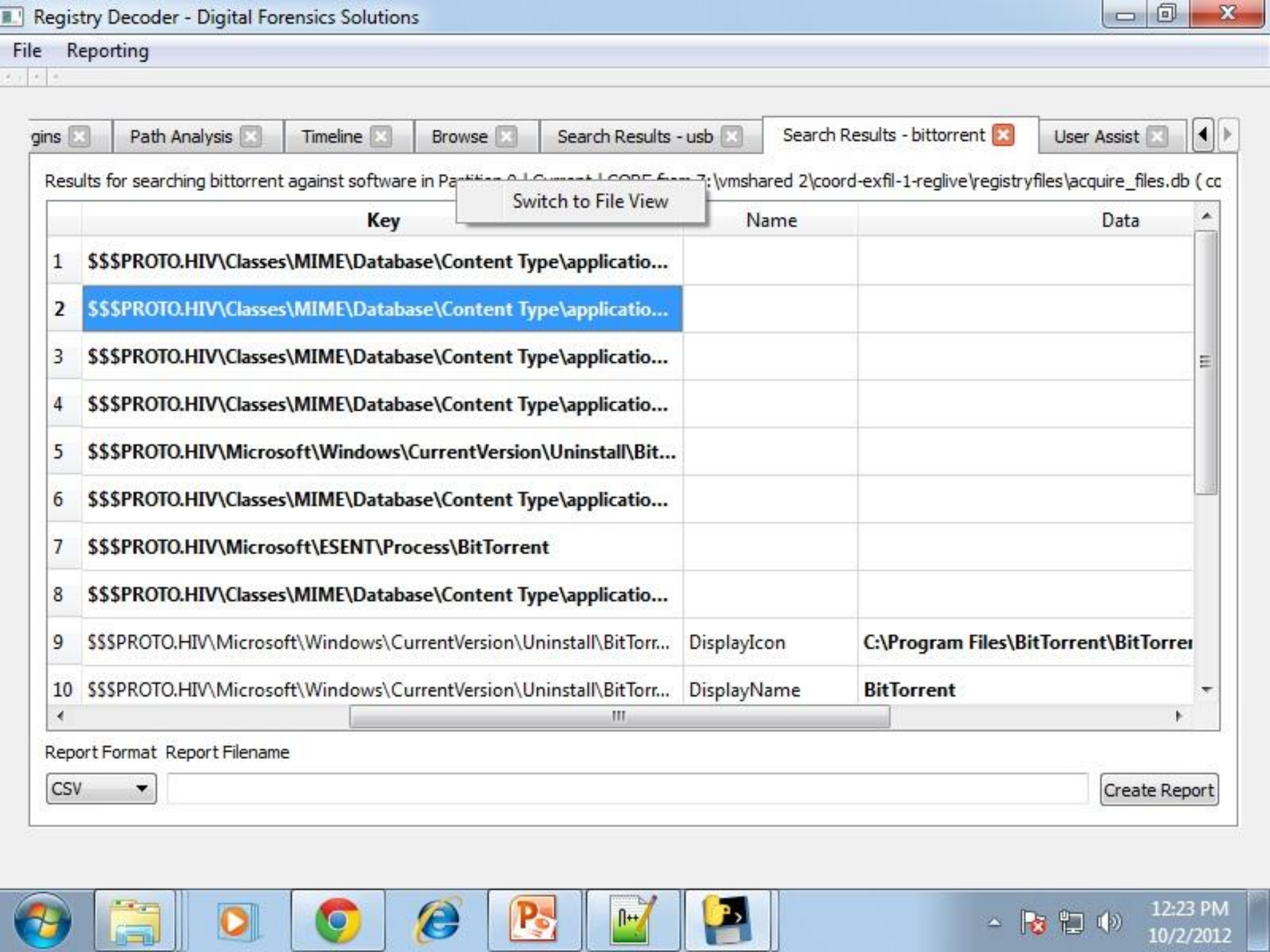
Advanced Search

- There are currently no good tool for mass searching across registry hives (right?)
  - F3, per-hive, context-less indexed search
- RD allows users to quickly search for a single term or a collection of terms (from a file) across any selected hives in a case
- This can quickly point to areas of interest
  - Users can jump from a search result key to a "browse" view of that key in its hive
    - Gives immediate context

Advanced Search (cont.)

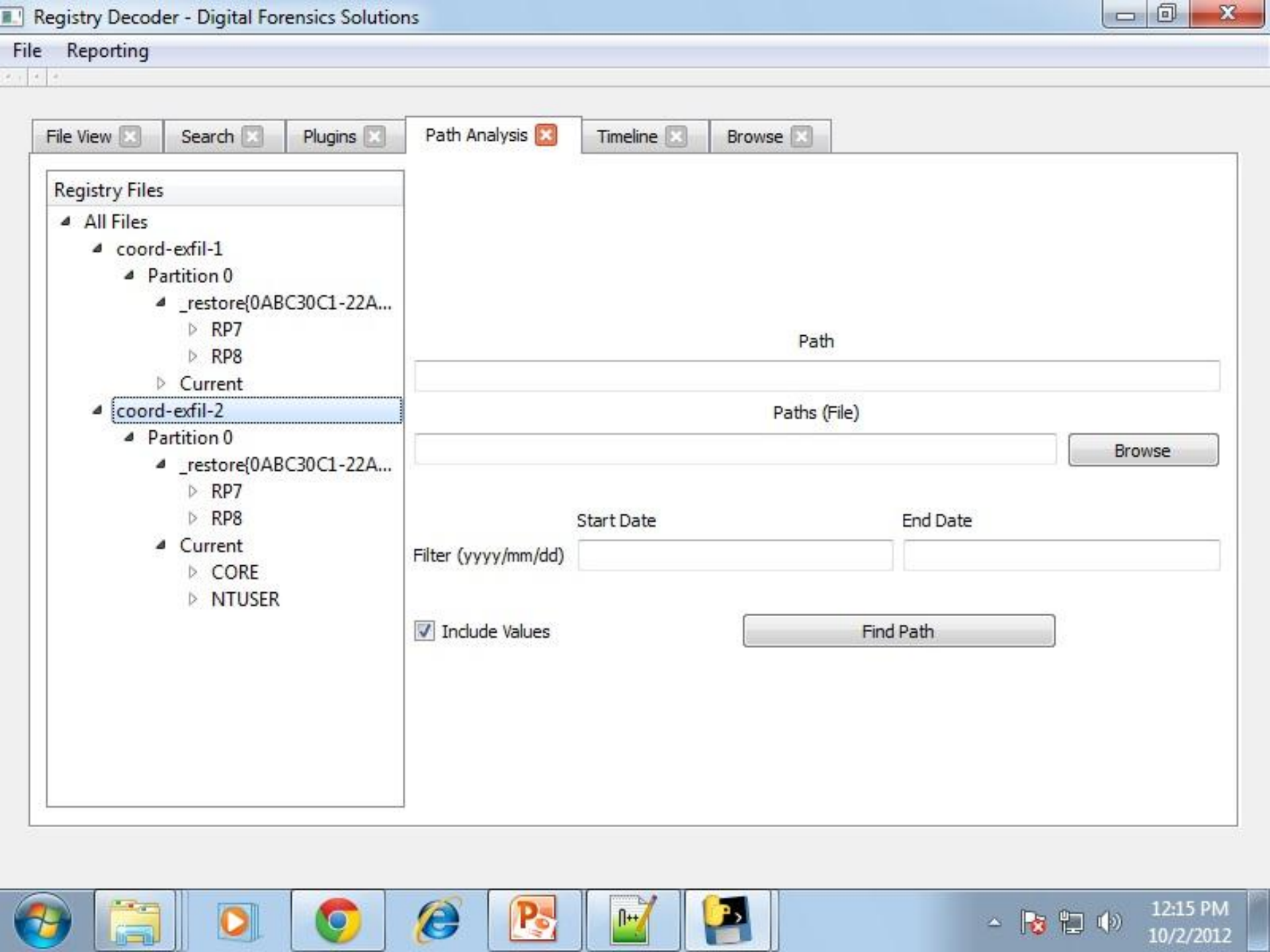
- Can limit searches by:
  - Exact or partial matching
  - Wildcard matching (*, ?)
  - Search across any combination of
    - Key name
    - Value name
    - Value data
  - Filter results by start date and end date using last write time of keys
- Matching key/name/data bolded


Registry Decoder - Digital Forensics Solutions
File
Reporting
File View
Search
Plugins
Path Analysis
Timeline
Browse
Registry Files
All Files
coord-exfil-1
Partition 0
_restore{0ABC30C1-22A7-4F03-8BD5-291E55749347}
RP7
CORE
SAM
SECURITY
SOFTWARE
SYSTEM
NTUSER
RP8
Current
CORE
default
SAM
SECURITY
software
system
NTUSER
coord-exfil-2
Search Term
Search Terms (File)
Browse
Exact Search
Partial Search
Keys
Names
Data
Start Date
End Date
Filter (yyyy/mm/dd)
Perform Diff
Search
12:10 PM
10/2/2012


Registry Decoder - Digital Forensics Solutions
File
Reporting
gins
Path Analysis
Timeline
Browse
Search Results - usb
Search Results - bittorrent
User Assist
Results for searching bittorrent against software in Pa :\vmshared 2\coord-exfil-1-reglive\registryfiles\acquire_files.db (cc
Switch to File View
Key
Name
Data
1 $$$PROTO.HIV\Classes\MIME\Database\Content Type\applicatio...
2 $$$PROTO.HIV\Classes\MIME\Database\Content Type\applicatio...
3 $$$PROTO.HIV\Classes\MIME\Database\Content Type\applicatio...
4 $$$PROTO.HIV\Classes\MIME\Database\Content Type\applicatio...
5 $$$PROTO.HIV\Microsoft\Windows\CurrentVersion\Uninstall\Bit...
6 $$$PROTO.HIV\Classes\MIME\Database\Content Type\applicatio...
7 $$$PROTO.HIV\Microsoft\ESENT\Process\BitTorrent
8 $$$PROTO.HIV\Classes\MIME\Database\Content Type\applicatio...
9 $$$PROTO.HIV\Microsoft\Windows\CurrentVersion\Uninstall\BitTorr... DisplayIcon C:\Program Files\BitTorrent\BitTorre
10 $$$PROTO.HIV\Microsoft\Windows\CurrentVersion\Uninstall\BitTorr... DisplayName BitTorrent
Report Format
Report Filename
CSV
Create Report
12:23 PM
10/2/2012

Path-Based Analysis

- Given a path and a set of hive files, generates output tabs for each file containing the path
- Example:
  - To search for: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes
  - And not receive other “PersistentRoutes” results
- Quickly determine if a path exists in a set of files
  - No clicking through 20 levels of keys (per file)
  - Hits can be exported with associated values
  - No extraneous results as in search

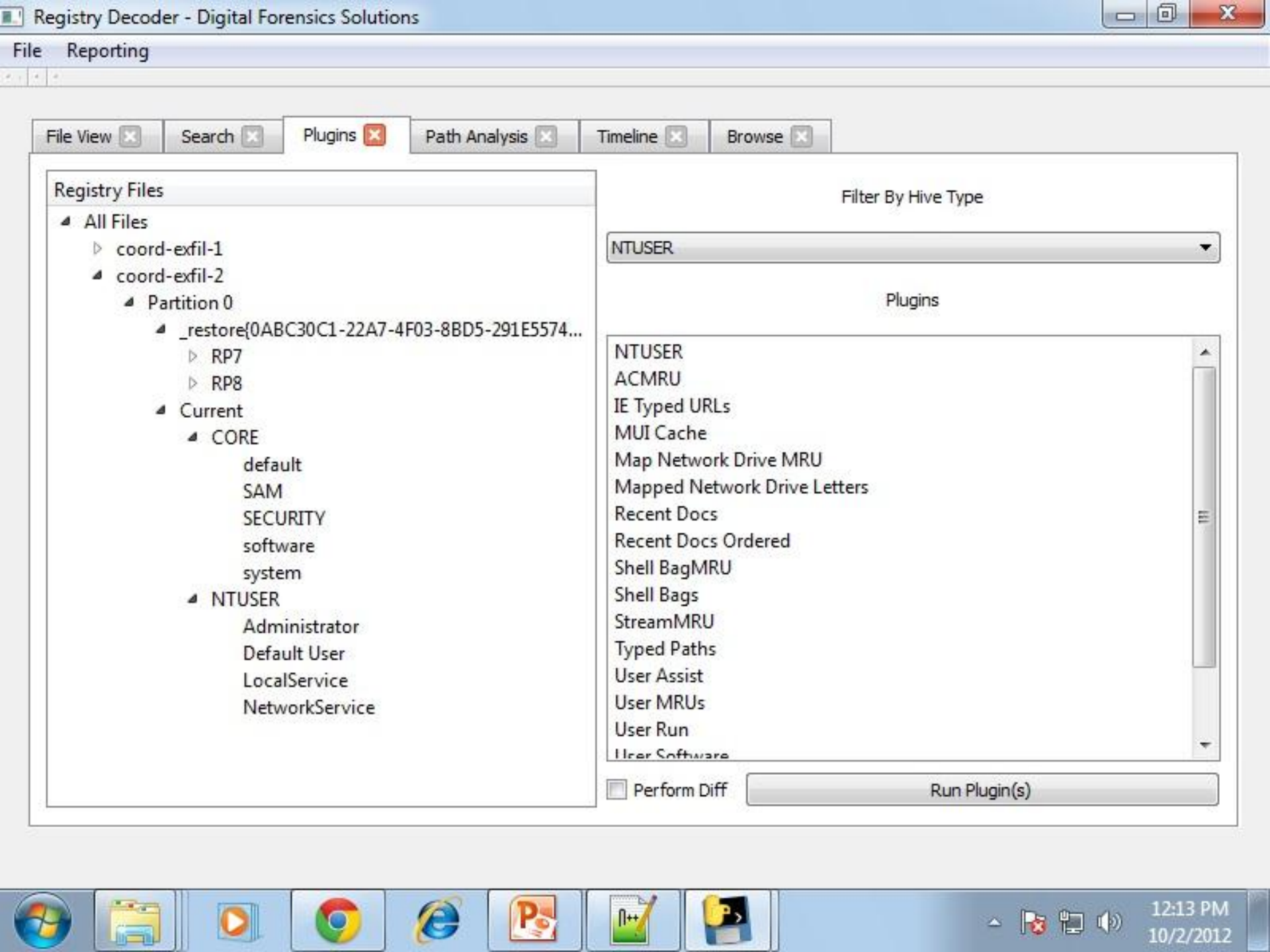

Registry Decoder - Digital Forensics Solutions
File
Reporting
File View
Search
Plugins
Path Analysis
Timeline
Browse
Registry Files
All Files
coord-exfil-1
Partition 0
_restore{0ABC30C1-22A...
RP7
RP8
Current
coord-exfil-2
Partition 0
_restore{0ABC30C1-22A...
RP7
RP8
Current
CORE
NTUSER
Path
Paths (File)
Browse
Start Date
End Date
Filter (yyyy/mm/dd)
Include Values
Find Path
12:15 PM
10/2/2012

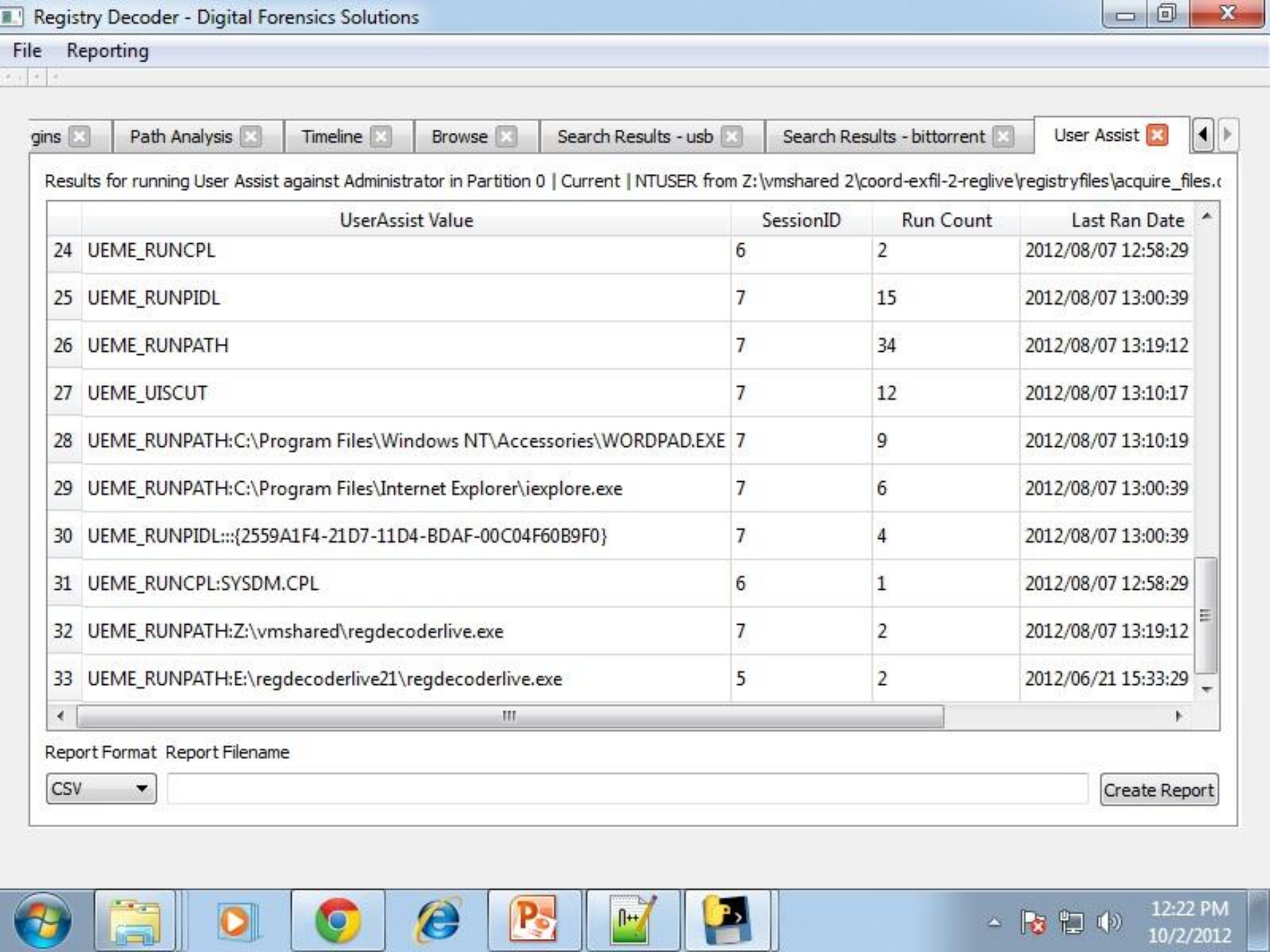
Using Path-Based Analysis

- Two interesting uses based on the files we select:
  - Multiple backups from same machine to determining when something hit the system
  - Hives from multiple machines to determining how far something has spread
- Specific software packages (including malware):
  - Determine if an application is installed
  - Key values may contain install date, install path, software, where downloads are stored, shared directories, etc.
  - AV vendors have data mapping unique keys -> malware
  - To test if malware has infected a set of machines, load the paths of keys of interest into RD and search

Plugins

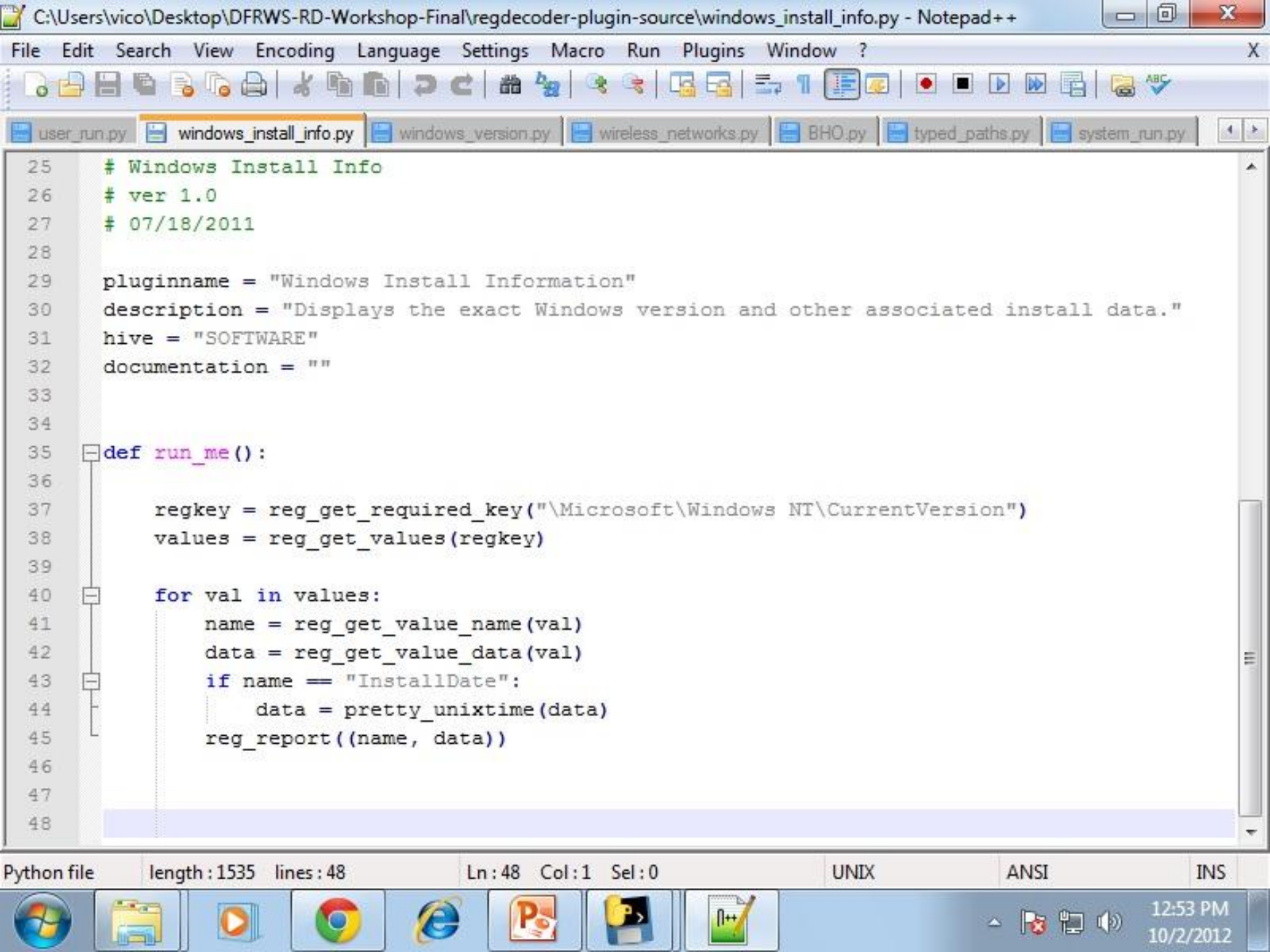
- The plugin system allows for targeted analysis of specific data within the registry
  - Mostly robbed from *regripper*
- For fixed analysis that must be done repeatedly
  - Listing MRU documents
  - UserAssist
- All plugins are in Python (bite me, Perl!)
- We provide an API designed to make plugin development as painless as possible
- Many plugins are less than 10 lines of code


Registry Decoder - Digital Forensics Solutions
File
Reporting
File View
Search
Plugins
Path Analysis
Timeline
Browse
Registry Files
All Files
coord-exfil-1
coord-exfil-2
Partition 0
_restore{0ABC30C1-22A7-4F03-8BD5-291E5574...
RP7
RP8
Current
CORE
default
SAM
SECURITY
software
system
NTUSER
Administrator
Default User
LocalService
NetworkService
Filter By Hive Type
NTUSER
Plugins
NTUSER
ACMRU
IE Typed URLs
MUI Cache
Map Network Drive MRU
Mapped Network Drive Letters
Recent Docs
Recent Docs Ordered
Shell BagMRU
Shell Bags
StreamMRU
Typed Paths
User Assist
User MRUs
User Run
Perform Diff
Run Plugin(s)
12:13 PM
10/2/2012


Registry Decoder - Digital Forensics Solutions
File
Reporting
gins
Path Analysis
Timeline
Browse
Search Results - usb
Search Results - bittorrent
User Assist
Results for running User Assist against Administrator in Partition 0 | Current | NTUSER from Z:\vmshared 2\coord-exfil-2-reglive\registryfiles\acquire_files.
UserAssist Value
SessionID
Run Count
Last Ran Date
24 UEME_RUNCPL 6 2 2012/08/07 12:58:29
25 UEME_RUNPIDL 7 15 2012/08/07 13:00:39
26 UEME_RUNPATH 7 34 2012/08/07 13:19:12
27 UEME_UISCUT 7 12 2012/08/07 13:10:17
28 UEME_RUNPATH:C:\Program Files\Windows NT\Accessories\WORDPAD.EXE 7 9 2012/08/07 13:10:19
29 UEME_RUNPATH:C:\Program Files\Internet Explorer\iexplore.exe 7 6 2012/08/07 13:00:39
30 UEME_RUNPIDL:::{2559A1F4-21D7-11D4-BDAF-00C04F60B9F0} 7 4 2012/08/07 13:00:39
31 UEME_RUNCPL:SYSDM.CPL 6 1 2012/08/07 12:58:29
32 UEME_RUNPATH:Z:\vmshared\regdecoderlive.exe 7 2 2012/08/07 13:19:12
33 UEME_RUNPATH:E:\regdecoderlive21\regdecoderlive.exe 5 2 2012/06/21 15:33:29
Report Format
Report Filename
CSV
Create Report
12:22 PM
10/2/2012

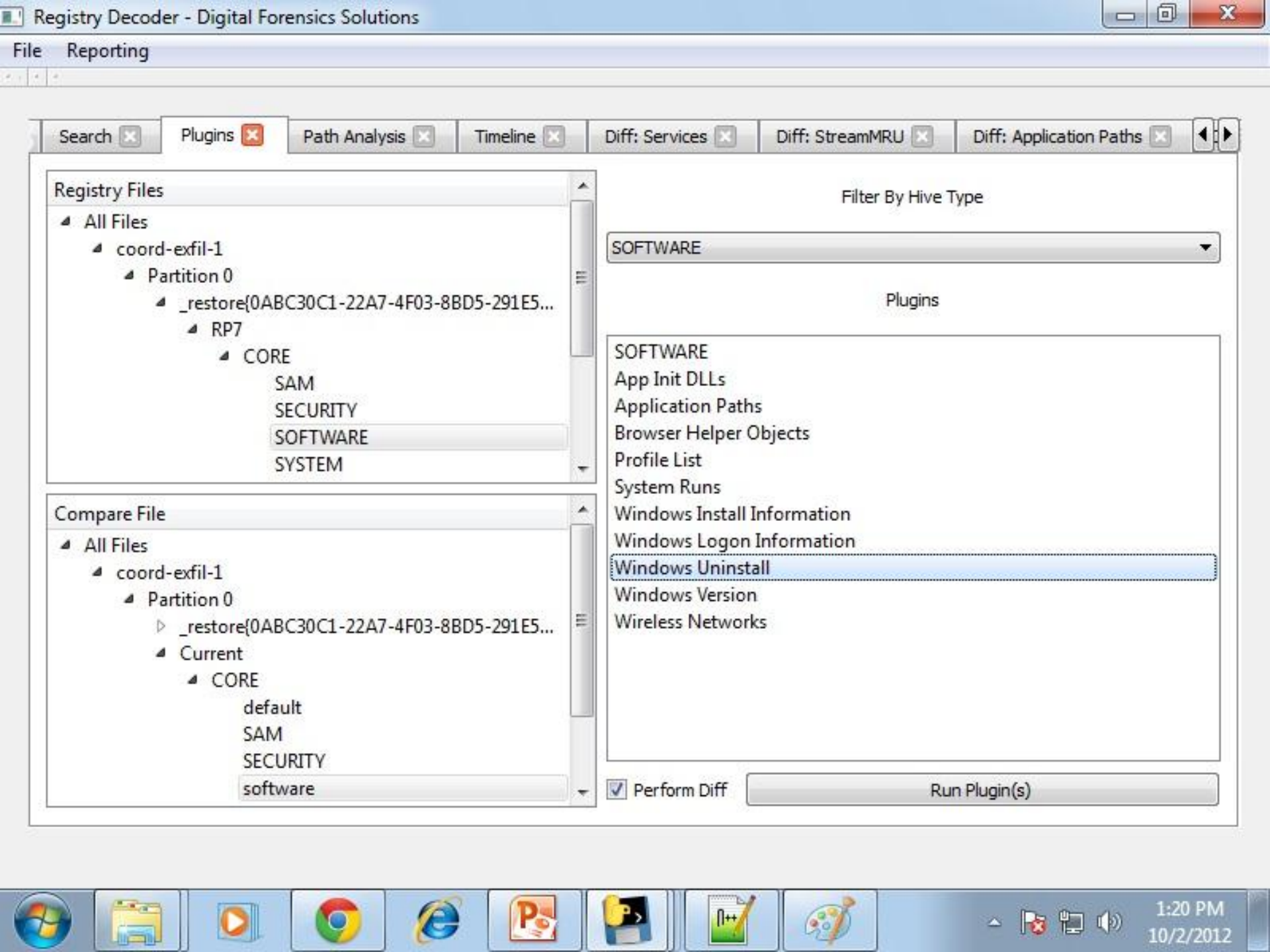
Writing Plugins

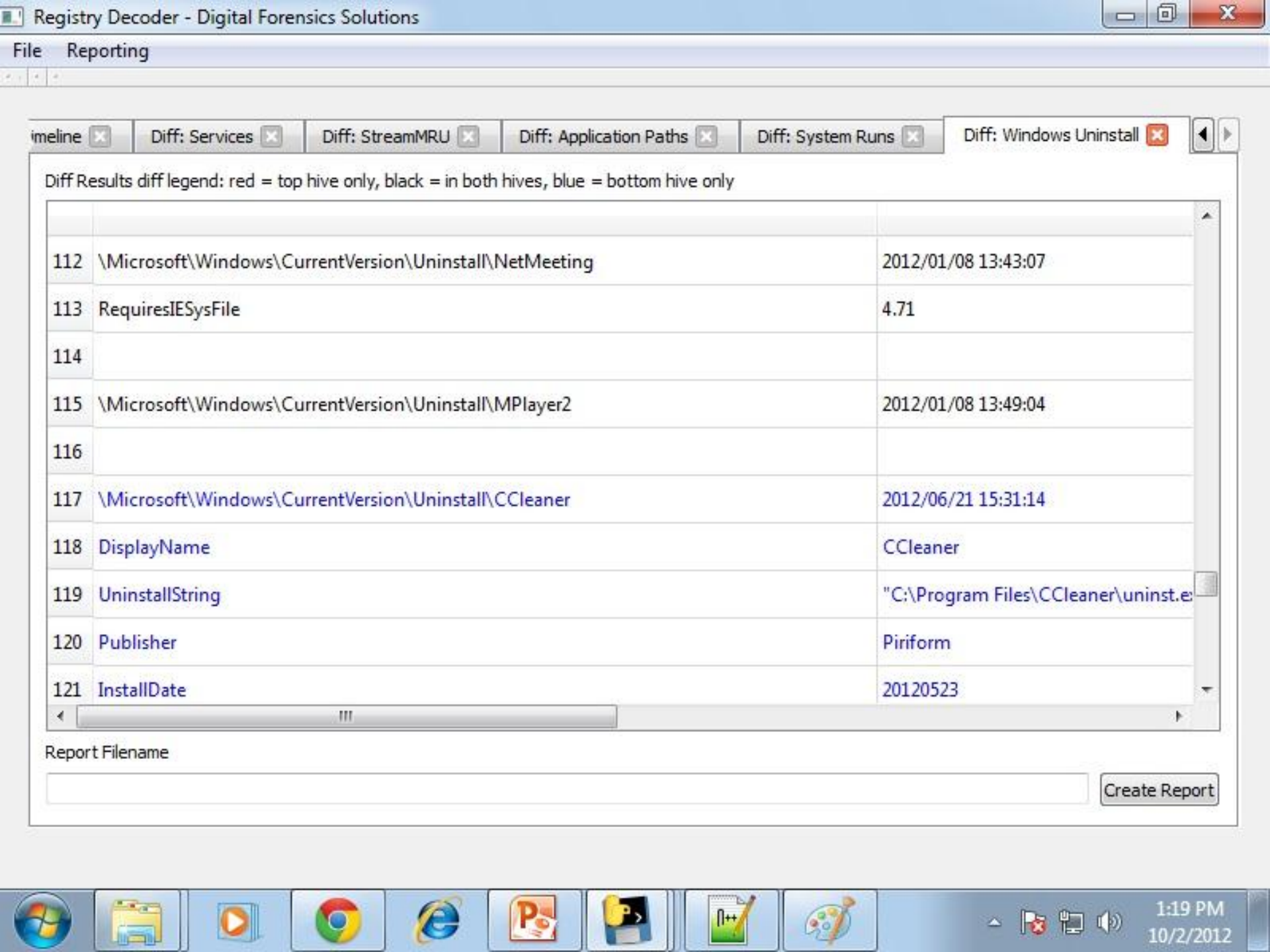
- There is a well-defined API to help you write plugins
  - See RegDecoder_API_DOC_v1.1
  - I wrote it, so of course it's "well-defined"
- Only about a 20 functions
  - Get a key given a path
  - Get a key's list of subkeys or values
  - Report results
  - Helper functions for time decoding, cc set
  - We should just look at a simple plugin …


C:\Users\vico\Desktop\DFRWS-RD-Workshop-Final\regdecoder-plugin-source\windows_install_info.py - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
user_run.py
windows_install_info.py
windows_version.py
wireless_networks.py
BHO.py
typed_paths.py
system_run.py
# Windows Install Info
# ver 1.0
# 07/18/2011
pluginname = "Windows Install Information"
description = "Displays the exact Windows version and other associated install data."
hive = "SOFTWARE"
documentation = ""
def run_me():
regkey = reg_get_required_key("\Microsoft\Windows NT\CurrentVersion")
values = reg_get_values(regkey)
for val in values:
name = reg_get_value_name(val)
data = reg_get_value_data(val)
if name == "InstallDate":
data = pretty_unixtime(data)
reg_report((name, data))
Python file length : 1535 lines : 48 Ln : 48 Col : 1 Sel : 0 UNIX ANSI INS
12:53 PM
10/2/2012

Differencing

- Performed on two types of data:
  - Search results
  - Plugins output
- Shows differences in two specific instances of one of the two above types
  - E.g. differences between 2 sets of search results
- Results are shown in color-coded output:
  - Red means the results are only in the first
  - Black means both
  - Blue means only the second


Registry Decoder - Digital Forensics Solutions
File
Reporting
Search
Plugins
Path Analysis
Timeline
Diff: Services
Diff: StreamMRU
Diff: Application Paths
Registry Files
All Files
coord-exfil-1
Partition 0
_restore{0ABC30C1-22A7-4F03-8BD5-291E5...
RP7
CORE
SAM
SECURITY
SOFTWARE
SYSTEM
Compare File
All Files
coord-exfil-1
Partition 0
_restore{0ABC30C1-22A7-4F03-8BD5-291E5...
Current
CORE
default
SAM
SECURITY
software
Filter By Hive Type
SOFTWARE
Plugins
SOFTWARE
App Init DLLs
Application Paths
Browser Helper Objects
Profile List
System Runs
Windows Install Information
Windows Logon Information
Windows Uninstall
Windows Version
Wireless Networks
Perform Diff
Run Plugin(s)
1:20 PM
10/2/2012


Registry Decoder - Digital Forensics Solutions
File
Reporting
imeline
Diff: Services
Diff: StreamMRU
Diff: Application Paths
Diff: System Runs
Diff: Windows Uninstall
Diff Results diff legend: red = top hive only, black = in both hives, blue = bottom hive only
112 \Microsoft\Windows\CurrentVersion\Uninstall\NetMeeting 2012/01/08 13:43:07
113 RequiresIESysFile 4.71
114
115 \Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2 2012/01/08 13:49:04
116
117 \Microsoft\Windows\CurrentVersion\Uninstall\CCleaner 2012/06/21 15:31:14
118 DisplayName CCleaner
119 UninstallString "C:\Program Files\CCleaner\uninst.e
120 Publisher Piriform
121 InstallDate 20120523
Report Filename
Create Report
1:19 PM
10/2/2012

Differencing Over Time

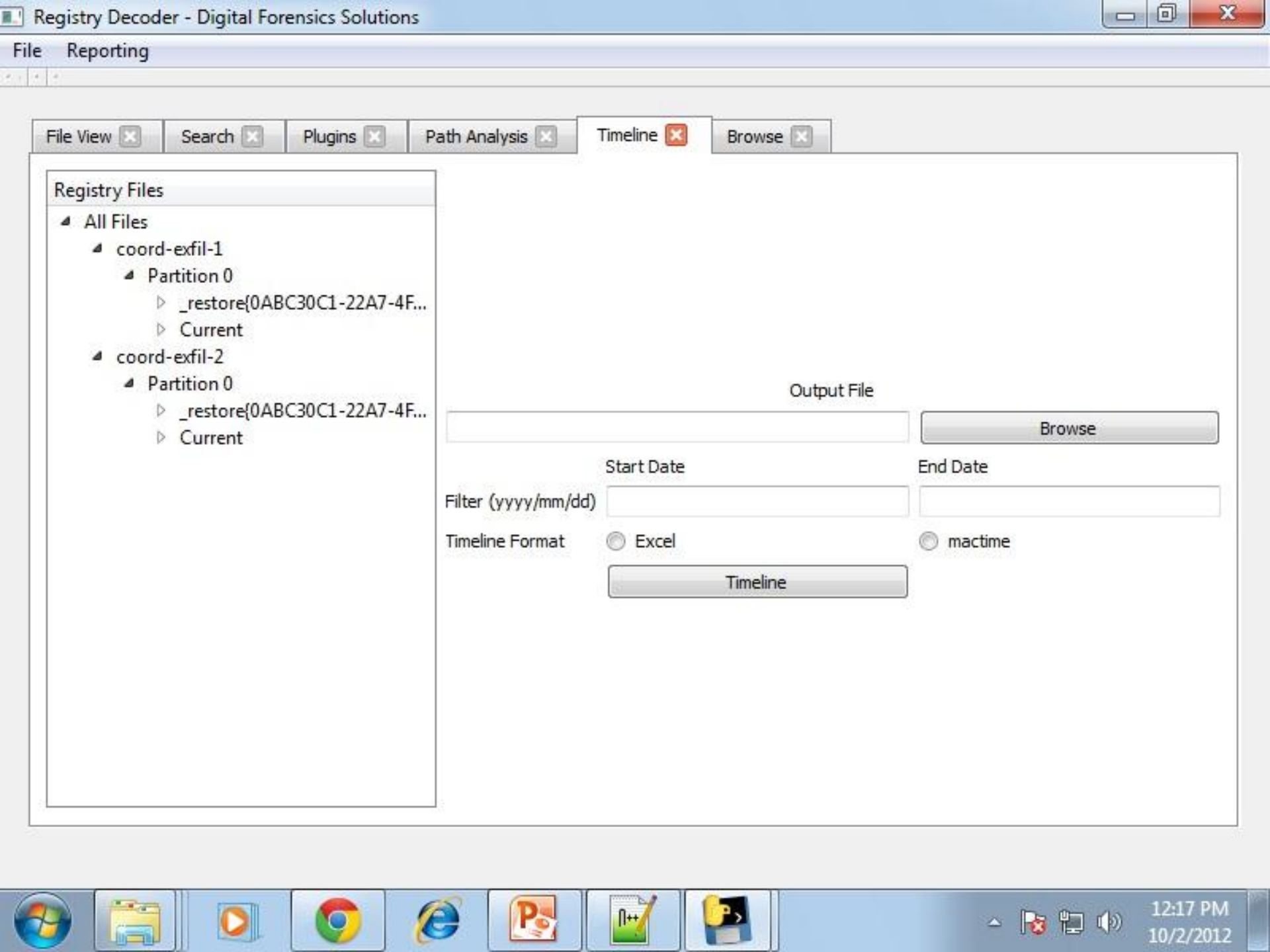
- Can quickly highlight what events occurred between two points in time
  - USBSTOR plugin will illustrate what new devices have been used since some previous registry backup (even if broken lastwrite)
  - Services plugin for a user will highlight what new services have been installed since some previous registry backup (malware)
- Think: analysis of current system versus a known baseline

Differencing Across Machines

- Can answer a number of interesting questions:
  - Was a USB device shared between 2 machines?
  - What set of users used any specific programs (malware, exfiltration, etc.)?
  - Were employees sharing documents?
- Useful when investigating collusion between employees or when a user has multiple computers

Timelineing

- Hives can be timelined based on the last write time of keys
- Included keys can be filtered by starting and/or ending time
- Output can be tab-separated (importable in Excel) or in Sleuth Kit *mactime* format
- Multiple input registry files can be processed into the same output timeline
- Useful in the face of timestomp?


Registry Decoder - Digital Forensics Solutions
File
Reporting
File View
Search
Plugins
Path Analysis
Timeline
Browse
Registry Files
All Files
coord-exfil-1
Partition 0
_restore{0ABC30C1-22A7-4F...
Current
coord-exfil-2
Partition 0
_restore{0ABC30C1-22A7-4F...
Current
Output File
Browse
Start Date
End Date
Filter (yyyy/mm/dd)
Timeline Format
Excel
mactime
Timeline
12:17 PM
10/2/2012

Reporting

- Because report writing is so much fun!
- Any table-based results can be exported
- This includes search results, plugins-generated data, timelines and difference reports
- Can also mass export all active analysis tabs
- Can filter results in individual tabs
- Output formats currently include:
  - HTML
  - PDF
  - XLS
  - CSV

Evidence File	Z:\vmshared 2\coord-exfil-1-reglive\registryfiles\acquire_files.db
Evidence Alias	coord-exfil-1
Registry File Group	Partition 0 | Current | CORE
Registry File	software
Analysis Type	Search
Search Term	bittorrent

Number	Last Write Time	Key	Name	Data
1	2012/01/09 11:45:46	$$$PROTO.HIV\Classes\MIME\Database\Content Type\application/x-bittorrentsearchdescription+xml		
2	2012/01/09 11:45:48	$$$PROTO.HIV\Classes\MIME\Database\Content Type\application/x-bittorrent-skin		
3	2012/01/09 11:45:48	$$$PROTO.HIV\Classes\MIME\Database\Content Type\application/x-bittorrent-key		
4	2012/01/09 11:45:48	$$$PROTO.HIV\Classes\MIME\Database\Content Type\application/x-bittorrent-app		

What's Next?

- More and more powerful plugins
- Command line support for scripting
- Support for pulling registry data from virtual machine RAM snapshots
- Performance enhancements
- And about 75 other things …
  - Deleted keys, better differencing, vmdk support, offline vss support, help us, .log, .sav, better unicode, …

Questions/Comments?

- Contact:
  - vico@digdeeply.com
  - registrydecoder@digdeeply.com

- Download RD:
  - digitalforensicssolutions.com/registrydecoder

Conclusion

- Registry Decoder provides a unified, open source system for registry analysis and research
  - Designed to handle multiple machines and
  - Multiple registry sets per machine
    - System Restore and VSS backups
  - Extensible via plugin system
  - Differencing engine
  - Powerful search