

A decorative graphic at the bottom of the slide features a grid pattern that tapers from left to right. The grid is overlaid with binary code (0s and 1s) in a light orange color. The background of the graphic is a mix of light and dark orange squares.

# Without a Trace:

Forensic Secrets for Windows Servers

BlackHat Windows 2004

Presented by Mark Burnett and James C. Foster

# Agenda

---

- Introduction
- Server Time Settings
- File Changes
- Tool Demo: Logz
- Recreating the Environment
- Memory Tricks
- Tracing the Steps
- Tool Demo: DatePilfer
- Tracking Program Installation
- Q&A

## Trivia Question

---

- In the Matrix Reloaded, after using NMap and SSHNuke to break in to the server, what does Trinity set as the new password?

\*Answers and prizes will be given out during the presentation

# Introduction

---

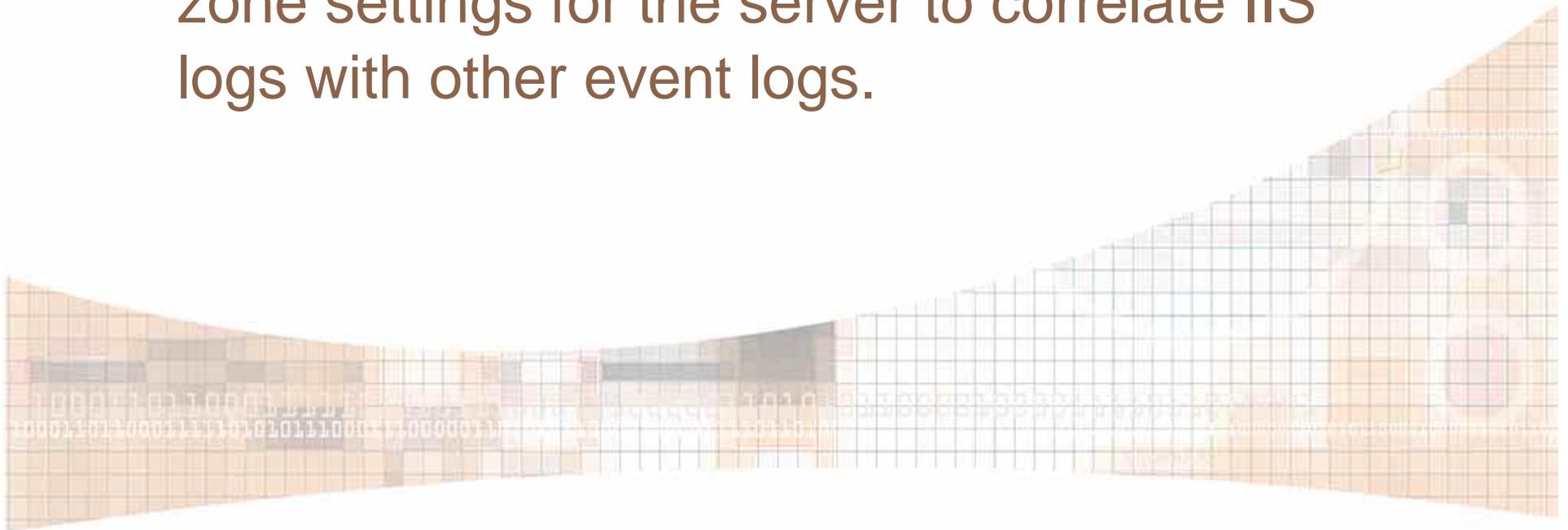
- Server forensics for security experts
- First responders vs. second responders
- Motivations and priorities
- Finding and preserving evidence
- Destroying evidence



# Server Time Settings

---

- Scenario: You have the IIS logs in a zip file but the server itself has since been reformatted and reinstalled.
- Problem: You must determine the time zone settings for the server to correlate IIS logs with other event logs.



# Server Time Settings

---

- Solution: Check the log file dates to get the time zone.

```
Directory of C:\Windows\System32\LogFiles\W3SVC1
```

```
09/27/2003  07:00 PM           1,461,370  ex030927.log
09/29/2003  07:00 PM             629,006  ex030929.log
09/30/2003  07:00 PM           1,134,950  ex030930.log
          3 File(s)           3,331,151 bytes
          2 Dir(s)  7,842,717,696 bytes free
```

- Tip: Creation date is when you extracted logs from the zip file
- Tip: Adjust for Daylight Saving
- Tip: Correlate with other event logs to check clock accuracy

# Question

---

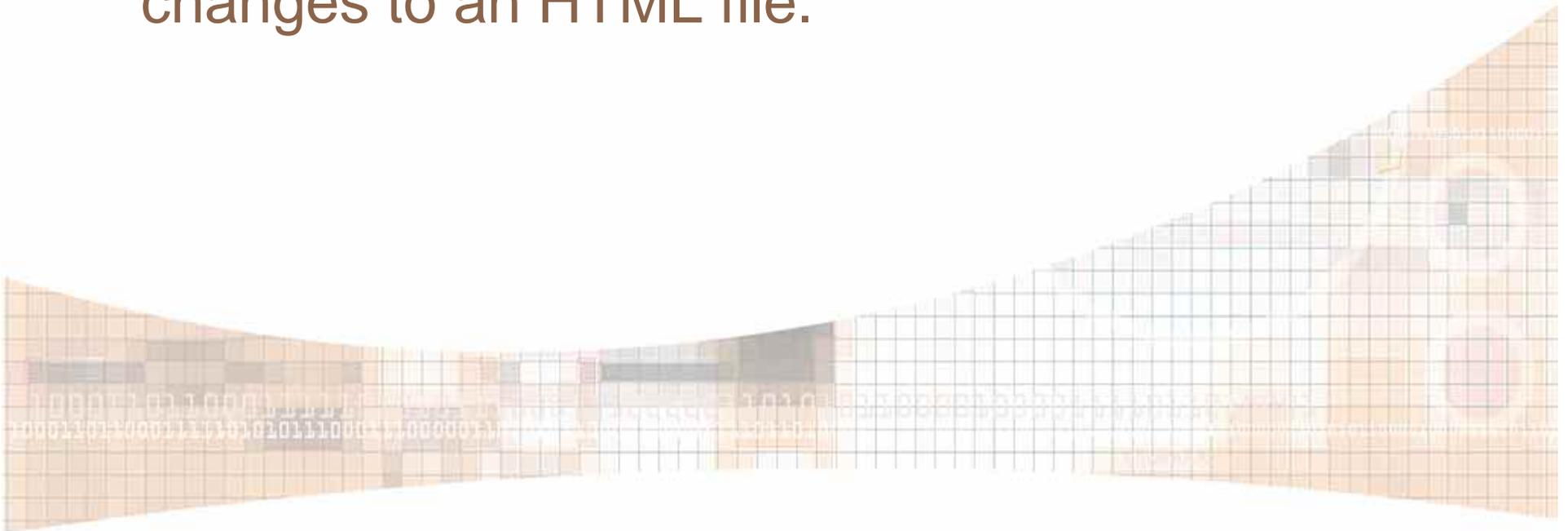
- What would cause an IIS log file to have continuous log entries from 0:00 through 23:59 (a full day) followed by more entries in that same log from 10:13 through 12:28?

\*Answers and prizes will be given out during the presentation

# File Changes

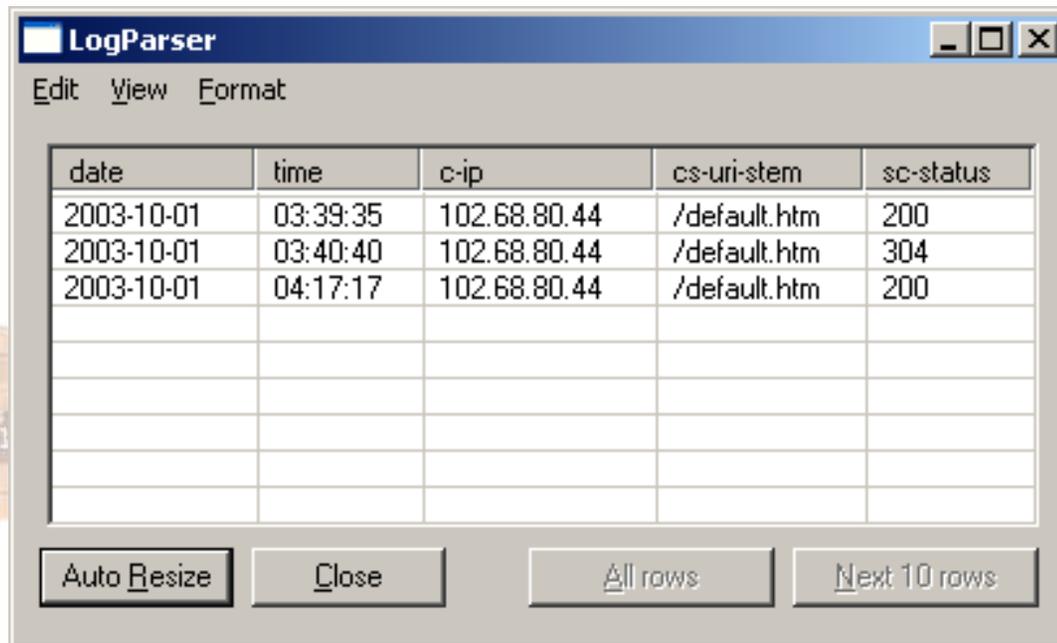
---

- Scenario: An HTML file in the web root contains malicious code and you need to track down when the changes occurred.
- Problem: You need to create a timeline of changes to an HTML file.



# File Changes

- Solution: Use LogParser to track down combinations of 200 and 304 status codes for the same IP address.
- ```
C:\>logparser "SELECT DISTINCT date, time, c-ip, cs-uri-stem, sc-status FROM ex031224.log WHERE c-ip in (SELECT DISTINCT c-ip FROM ex031224.log WHERE sc-status=304 AND cs-uri-stem='/default.htm') AND (sc-status=200 OR sc-status=304) AND cs-uri-stem='/default.htm' GROUP BY date, time, cs-uri-stem, c-ip, sc-status ORDER BY date, c-ip" -o:datagrid
```



The screenshot shows the LogParser application window. The title bar reads "LogParser". Below the title bar is a menu bar with "Edit", "View", and "Format". The main area contains a data grid with the following columns: "date", "time", "c-ip", "cs-uri-stem", and "sc-status". The grid contains three rows of data:

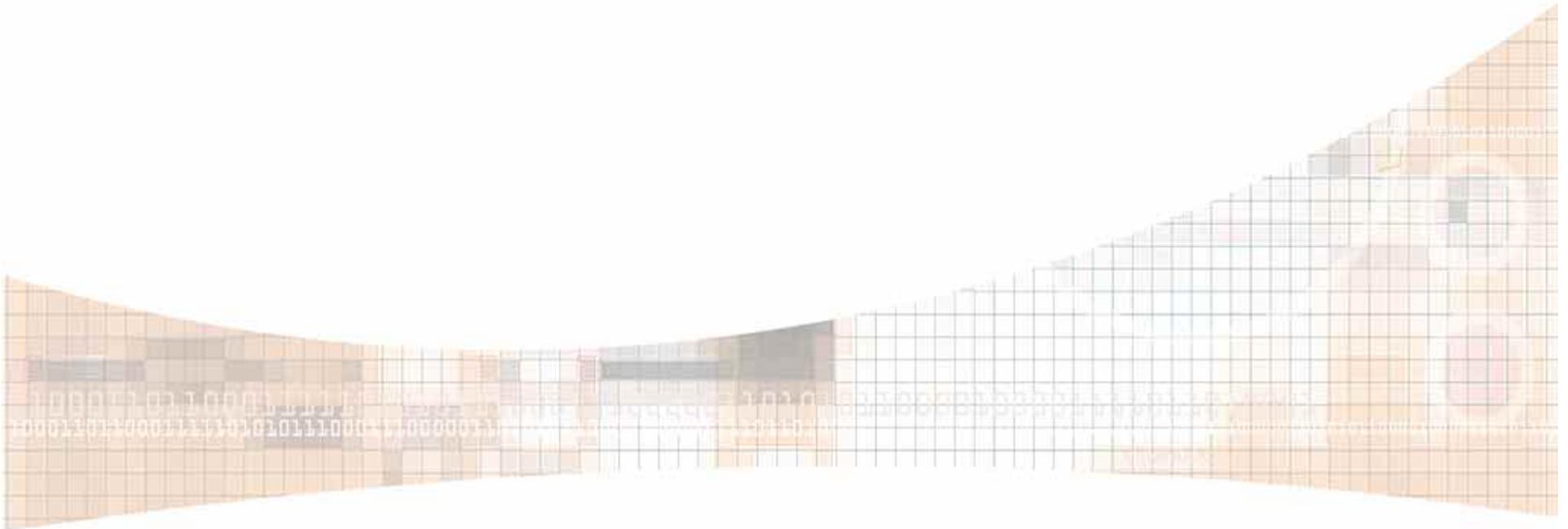
| date       | time     | c-ip         | cs-uri-stem  | sc-status |
|------------|----------|--------------|--------------|-----------|
| 2003-10-01 | 03:39:35 | 102.68.80.44 | /default.htm | 200       |
| 2003-10-01 | 03:40:40 | 102.68.80.44 | /default.htm | 304       |
| 2003-10-01 | 04:17:17 | 102.68.80.44 | /default.htm | 200       |

At the bottom of the window, there are four buttons: "Auto Resize", "Close", "All rows", and "Next 10 rows".

# File Changes

---

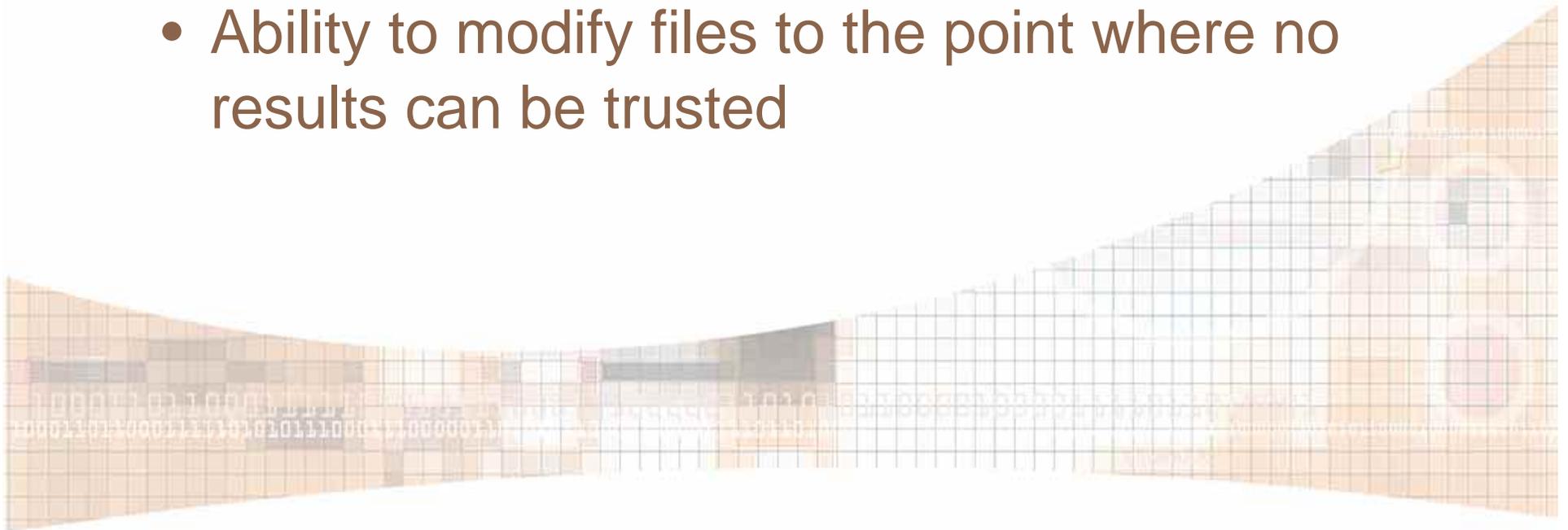
- Did you know?
  - Windows keeps an NTFS journal of all file changes. To view the journal in Windows XP or 2003 use the FSUTIL command.



# Live Tool Demo: Logz

---

- Drivers:
  - Some people may want the ability to quickly corrupt log files
  - Ability to cover up tracks
  - Ability to modify files to the point where no results can be trusted



# Live Tool Demo: Logz

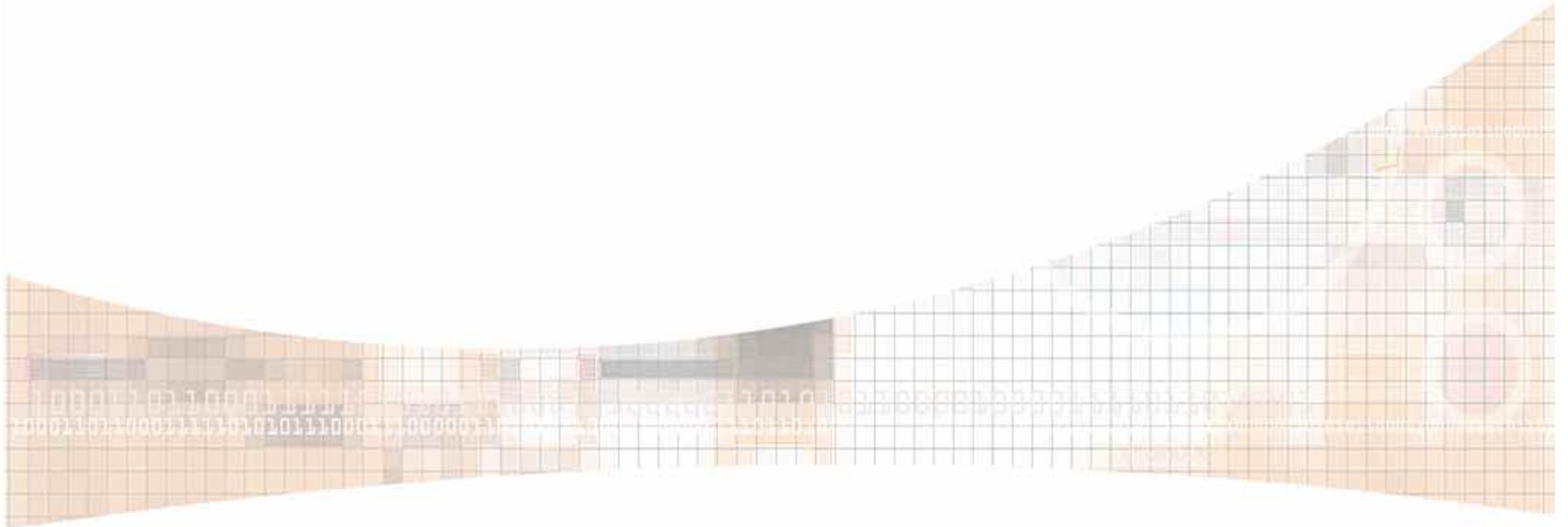
---

- Overview:
  - To be a one-stop-shop for all your needs in log modification, cleaning, and flooding
- Features (v1.0):
  - Ability to remove specified log entries
  - Ability to replace addresses in logs with a desired spoof address
  - Ability to replace addresses in logs with random addresses
  - Ability to randomly switch all addresses in logs
  - Ability to flood logs with bogus log entries

# Demo

---

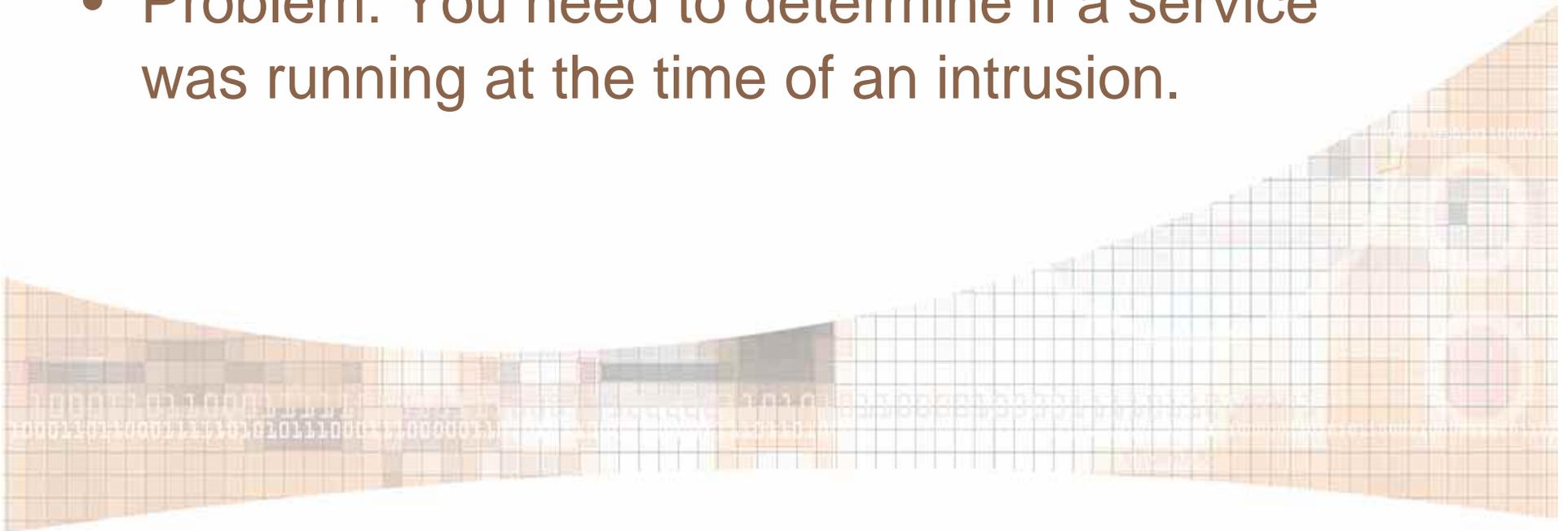
- 5 Min. Live Demo



# Recreating the Environment

---

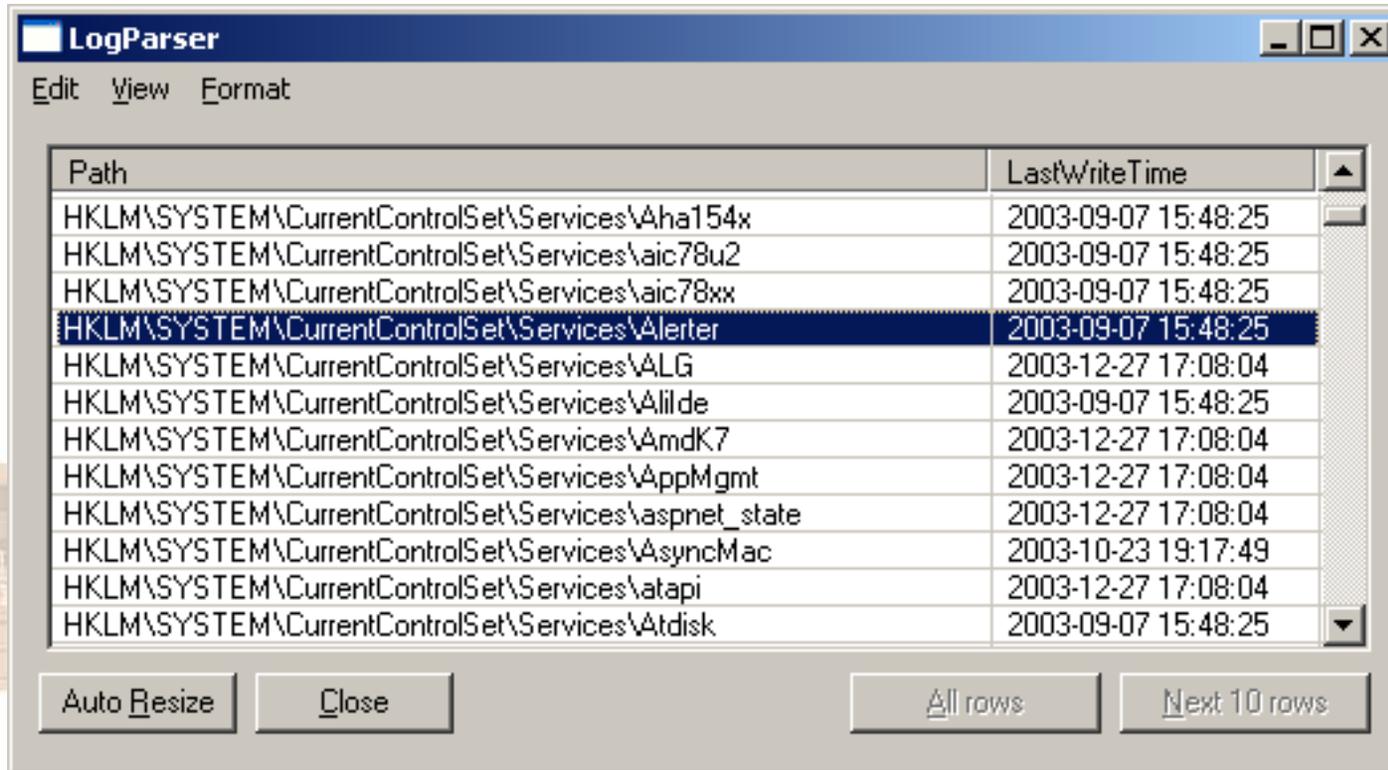
- Scenario: You know the date of an intrusion but not how they got in. You suspect they exploited an overflow in a Windows service but that service is no longer running.
- Problem: You need to determine if a service was running at the time of an intrusion.



# Recreating the Environment

- Solution: Use LogParser to determine when each service's startup mode last changed

```
C:\>logparser "SELECT Path, LastWriteTime FROM  
HKLM\SYSTEM\CurrentControlSet\Services\ WHERE ValueName='Start'" -e:-1  
-o:datagrid
```



The screenshot shows the LogParser application window with a menu bar (Edit, View, Format) and a table of results. The table has two columns: 'Path' and 'LastWriteTime'. The 'Alerter' service is highlighted in blue. At the bottom of the window, there are buttons for 'Auto Resize', 'Close', 'All rows', and 'Next 10 rows'.

| Path                                                | LastWriteTime       |
|-----------------------------------------------------|---------------------|
| HKLM\SYSTEM\CurrentControlSet\Services\Aha154x      | 2003-09-07 15:48:25 |
| HKLM\SYSTEM\CurrentControlSet\Services\aic78u2      | 2003-09-07 15:48:25 |
| HKLM\SYSTEM\CurrentControlSet\Services\aic78xx      | 2003-09-07 15:48:25 |
| HKLM\SYSTEM\CurrentControlSet\Services\Alerter      | 2003-09-07 15:48:25 |
| HKLM\SYSTEM\CurrentControlSet\Services\ALG          | 2003-12-27 17:08:04 |
| HKLM\SYSTEM\CurrentControlSet\Services\Alilde       | 2003-09-07 15:48:25 |
| HKLM\SYSTEM\CurrentControlSet\Services\AmdK7        | 2003-12-27 17:08:04 |
| HKLM\SYSTEM\CurrentControlSet\Services\AppMgmt      | 2003-12-27 17:08:04 |
| HKLM\SYSTEM\CurrentControlSet\Services\aspnet_state | 2003-12-27 17:08:04 |
| HKLM\SYSTEM\CurrentControlSet\Services\AsyncMac     | 2003-10-23 19:17:49 |
| HKLM\SYSTEM\CurrentControlSet\Services\atapi        | 2003-12-27 17:08:04 |
| HKLM\SYSTEM\CurrentControlSet\Services\Atdisk       | 2003-09-07 15:48:25 |

# Recreating the Environment

---

- Tip: Determine how long a process has been running using WMI (ProcessStarted.vbs)
- Tip: If an application saves registry settings on exit, the LastWriteTime will indicate the last time the application ran.

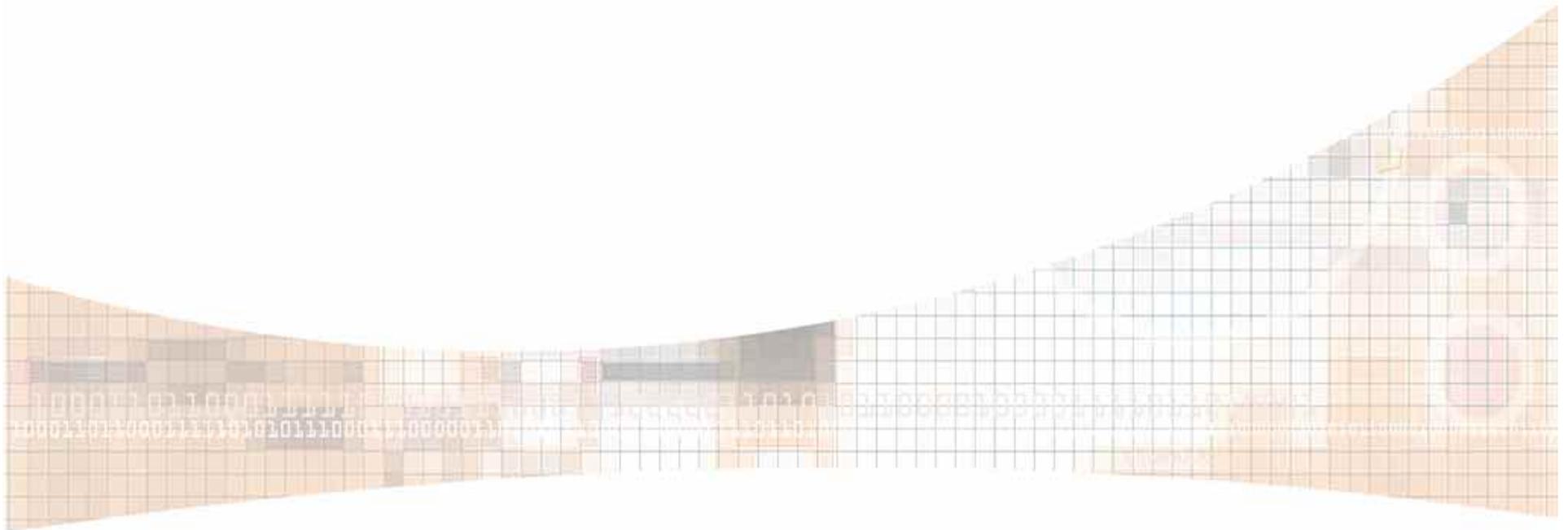


# Recreating the Environment

---

- Did you know?

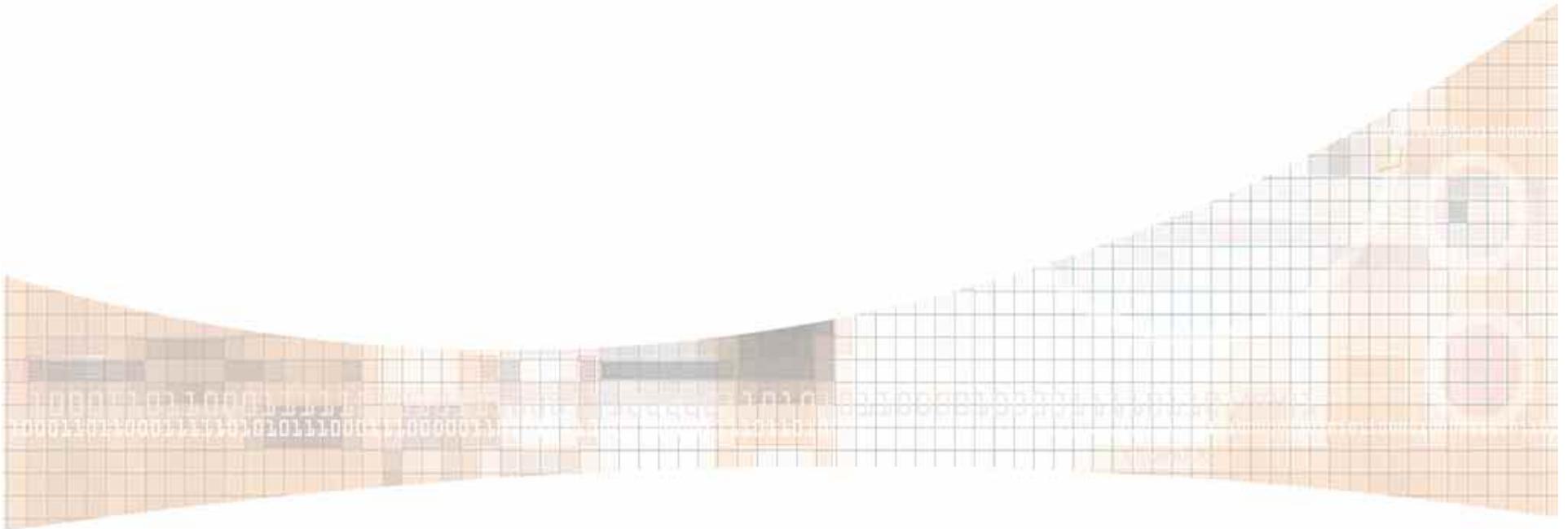
On Windows 2003 the scheduler service keeps a hidden log file at  
`c:\Windows\Tasks\schedlgu.txt`



# Determining Scope of Access

---

- Scenario: A hacker breaks into an e-commerce site and the credit card company needs to know exactly how much access he had.
- Problem: Determine type and level of access



# Determining Scope of Access

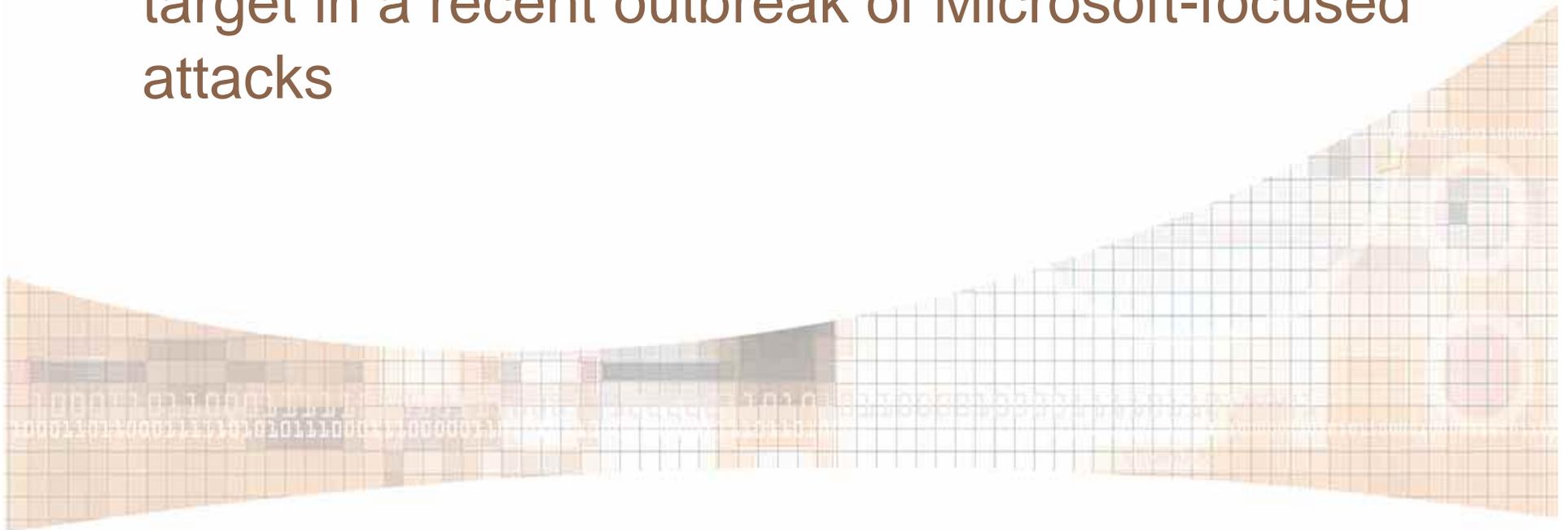
---

- Solution: Look for clues to indicate local console or terminal services access
  - Files in recycle bin
  - New user profile directories
  - Last modified dates on Start Menu icons
- Solution: Look for actions that require administrator-level access
  - Emptying the Event Log
  - Creating users
  - Other privileged access

# Memory Tricks

---

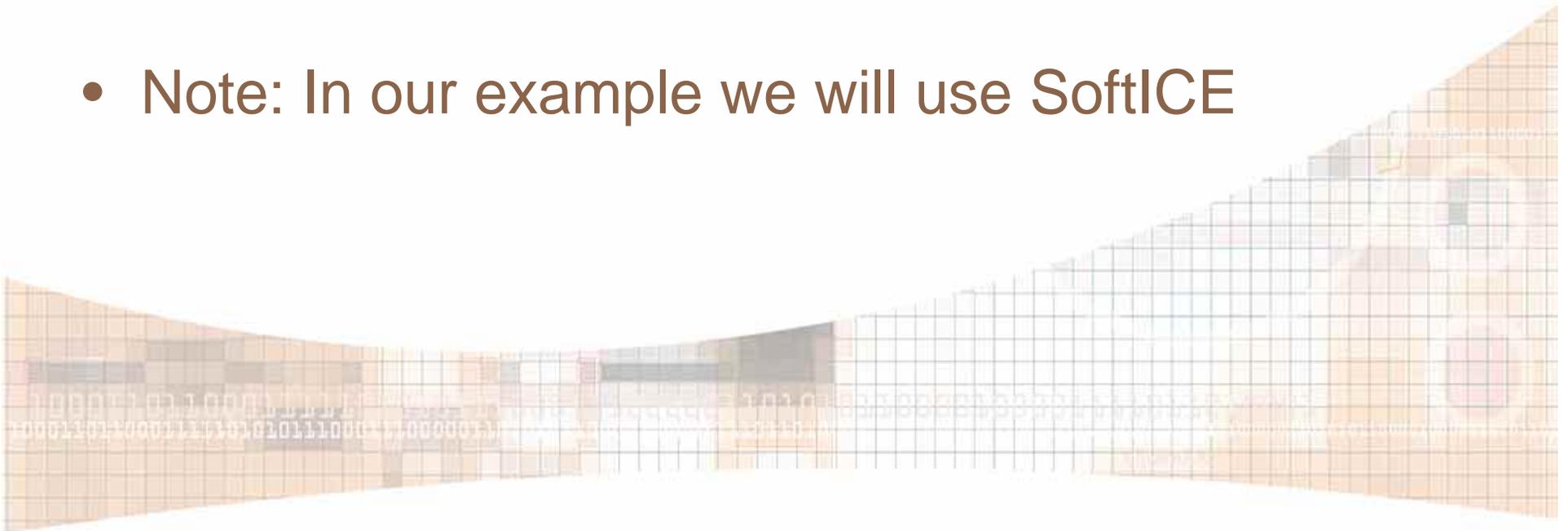
- Problem: You need to determine if a specific exploit has been run against your system
- Scenario: A publicly known vulnerable service has crashed and you believe you have been the target in a recent outbreak of Microsoft-focused attacks



# Memory Tricks

---

- Solution: Using just about any memory search tool you can look for the shellcode that would have been injected through the use of a publicly available exploit
- Note: In our example we will use SoftICE



# Memory Tricks

---

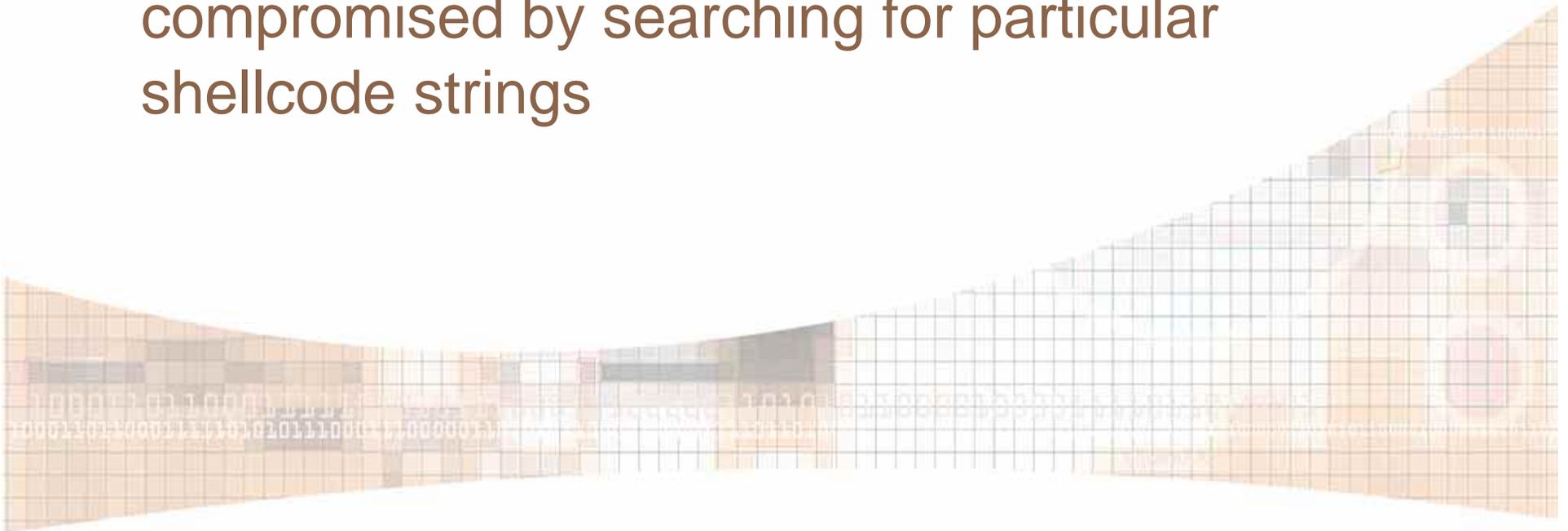
- Trivia Question:
  - In SoftICE what does the IRQ do?
- SoftICE Documentation:
- <http://frontline.compuware.com>



# Memory Tricks: Live Demo

---

- Exploit and Analysis Demo
- Overview: In our Case we will exploit a system then determine if our system has been compromised by searching for particular shellcode strings



## Question

---

- What kind of encryption is this using:  
HRZR\_EHACVQY:%pfvqy6%\Yvaxf\Tbbtyr.hey

\*Answers and prizes will be given out during  
the presentation

# Tracing the Steps

---

- Scenario: You know the hacker gained Terminal Services access but you need to know what he did after that.
- Problem: You must establish a timeline of events, file access, etc.



## Tracing the Steps

---

- Solution: Use LogParser to view lists of recent files from Documents and Settings

```
LogParser "SELECT LastWriteTime,  
CreationTime, Path INTO FileMRU.csv FROM  
'c:\documents and settings\*.*' WHERE Path  
LIKE '%recent%' AND Path NOT LIKE '%.'  
ORDER BY LastWriteTime DESC" -i:fs -  
recurse -o:csv
```

- Creates a .csv file you can open in Excel



# Tracing the Steps

---

- Solution: Use LogParser to find MRU

```
LogParser "SELECT Path, ValueName, Value,  
HEX_TO_ASC(Value) as Value2 INTO MRU-Lists.csv  
FROM \HKCU WHERE Path LIKE '%MRU%' OR Path LIKE  
'%recent%' OR Path LIKE '%Used%' OR Path LIKE  
'%Usage%' OR Path LIKE '%Time%' OR Path LIKE  
'%Date%' OR Path LIKE '%Last%' OR Path LIKE  
'%Updated%' OR Path LIKE '%History%' OR ValueName  
LIKE '%MRU%' OR ValueName LIKE '%recent%' OR  
ValueName LIKE '%Used%' OR ValueName LIKE  
'%Usage%' OR ValueName LIKE '%Time%' OR ValueName  
LIKE '%Date%' OR ValueName LIKE '%Last%' OR  
ValueName LIKE '%Updated%' OR ValueName LIKE  
'%History%' ORDER BY Path, ValueName" -o:csv
```

- Creates a .csv file you can open in Excel

# Tracing the Steps

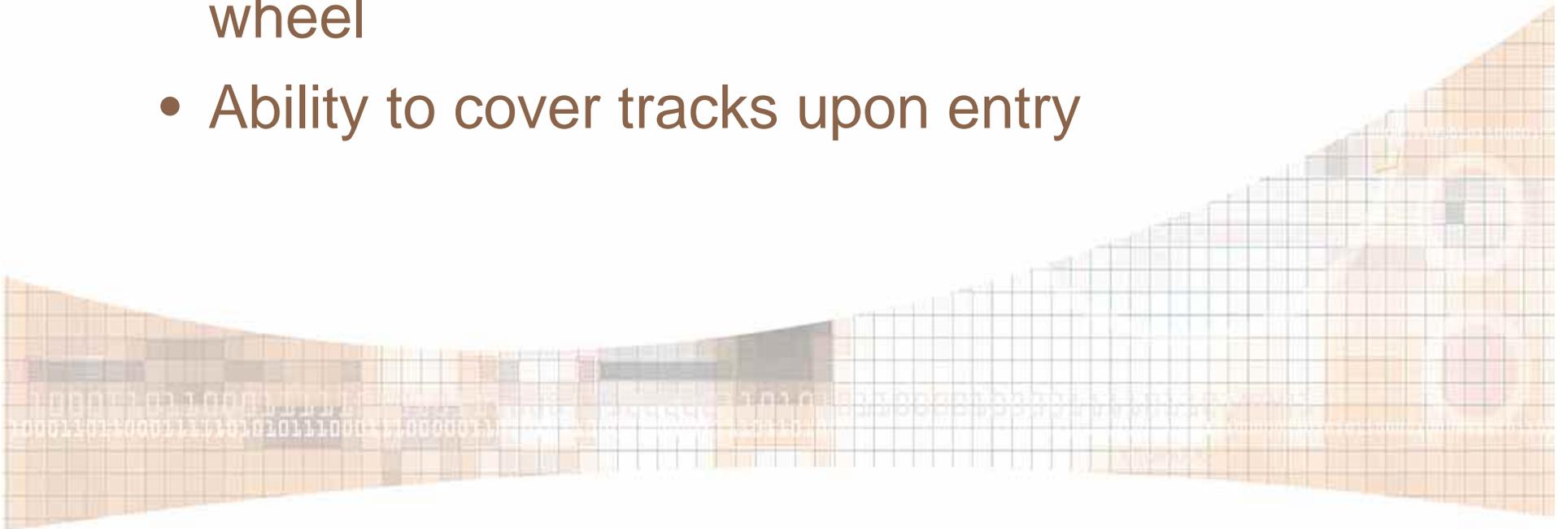
---

- Tip: Use LastWriteTime values on registry keys
  - Application Settings
  - OpenWith  
(HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts)
- Tip: Use UserAssist registry entries
- Tip: Open With last modified dates
- Tip: Don't overlook file modified and created dates.
- **Tip: Preventing MRU Lists**

# Live Tool Demo: Pilfer!

---

- Drivers:
  - Users want the ability to modify timestamps in bulk
  - Microsoft LogParser rocks, why recreate the wheel
  - Ability to cover tracks upon entry



# Live Tool Demo: Pilfer!

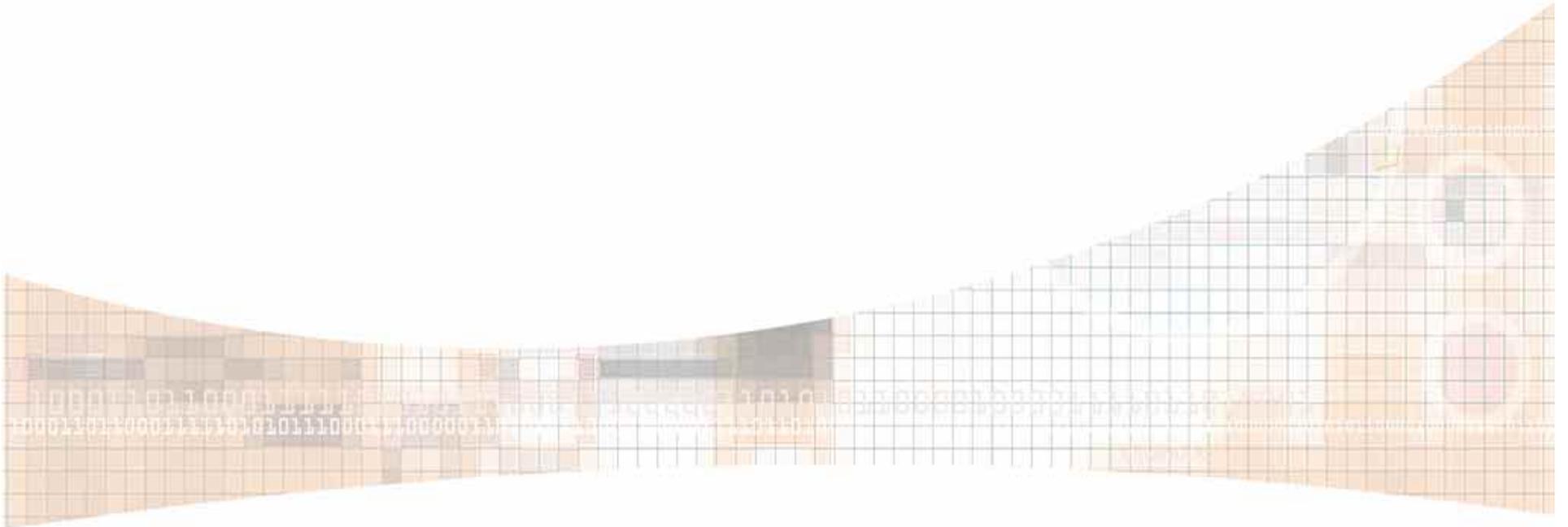
---

- Overview:
  - Pilfer is designed to be an easy-to-use tool for modifying mass amounts of filesystem timestamps
- Features (v1.0):
  - Initially designed to use Microsoft's LogParser output as input for file listings
  - Open API allows easy integration for other tools to pump in input
  - Ability to modify one/many file & directory timestamps serially
  - Ability to use specified or randomized timestamps

# Demo

---

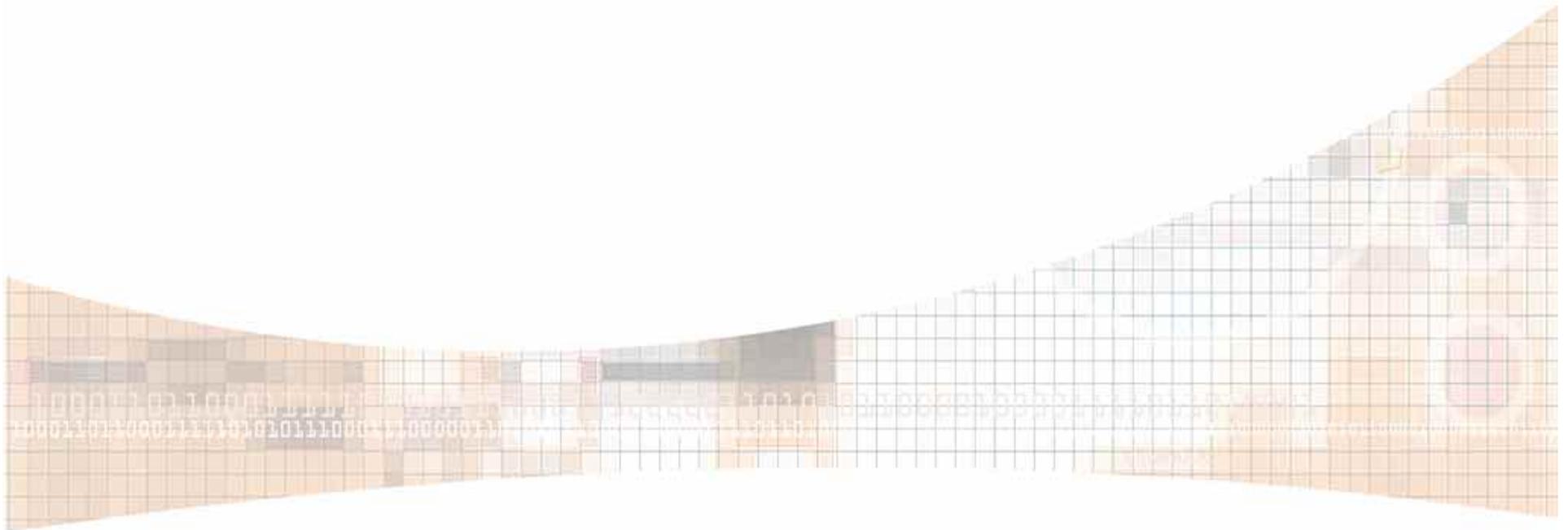
- 6-8 Min. Live Demo



# Program Installation

---

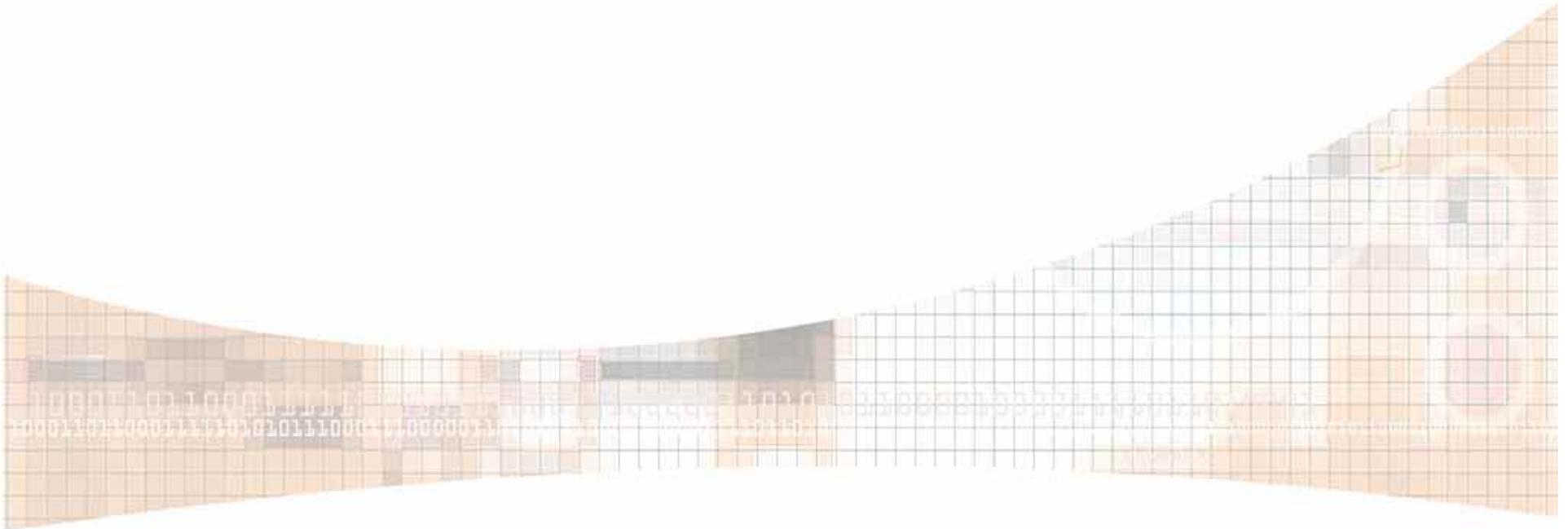
- Scenario: There are suspicious applications on a server and you don't know who installed what.
- Problem: Determine who installed which applications and when.



# Program Installation

---

- Solution: Check installation logs
- Solution: Check optional component logs
- Check registry
- Check file ownership



# Other Tools

---

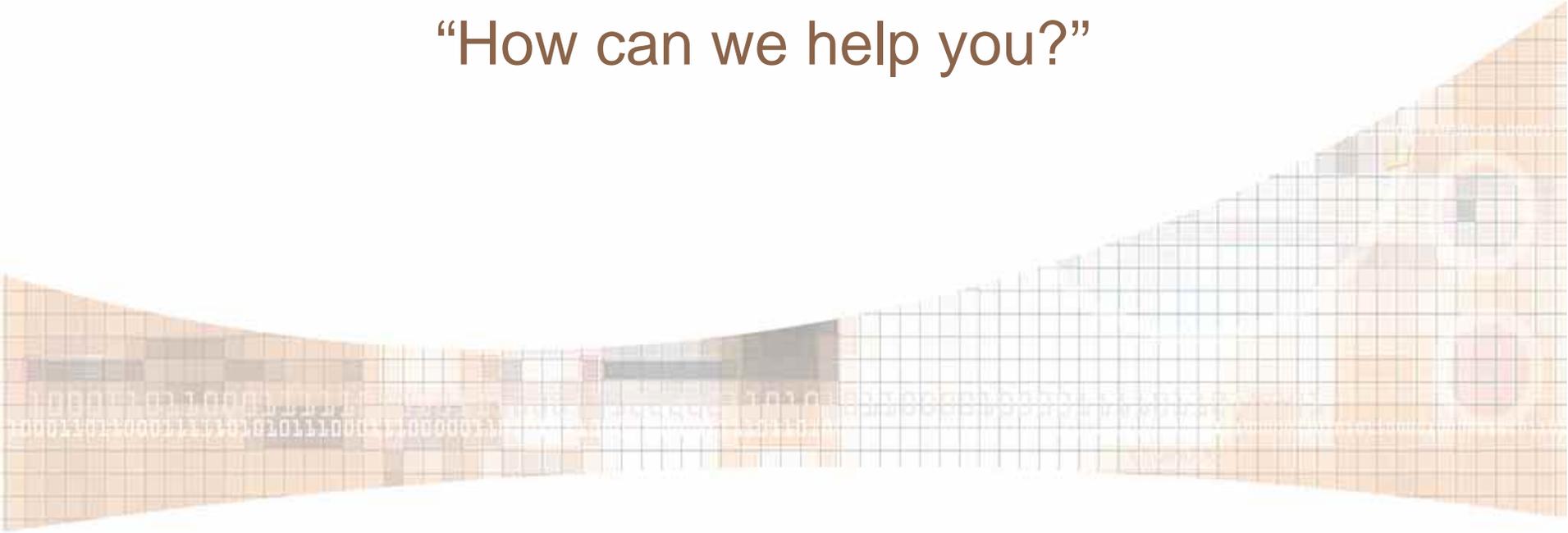
- LogParser - All-purpose query tool  
<http://download.microsoft.com>
- FavURLView - Shows details of internet shortcuts  
<http://www.digital-detective.co.uk/freetools/favurlview.asp>
- Decode - Date/time decoder  
<http://www.digital-detective.co.uk/freetools/decode.asp>
- Pasco - Index.dat viewer  
<http://www.foundstone.com/resources/proddesc/pasco.htm>
- Galleta - IE cookie tool  
<http://www.foundstone.com/resources/proddesc/galleta.htm>
- Rifiuti - Recycle bin tool  
<http://www.foundstone.com/resources/proddesc/rifiuti.htm>
- FSum - Fast file hasher  
<http://www.slavasoft.com/fsum/overview.htm>
- PMDump - Dump memory from a process  
<http://www.ntsecurity.nu/toolbox/pmdump/>

# The End

---

- Final Thoughts? Questions?

“How can we help you?”



# Contact Information:

---

Mark Burnett

[mb@xato.net](mailto:mb@xato.net)

James C. Foster

[jamesfoster@safe-mail.net](mailto:jamesfoster@safe-mail.net)

443.668.2527