SpectorSoft

Simplifying Employee Investigations

1.888.598.2788 | www.spectorsoft.com

Simplifying Employee Investigations

You just got news of yet *another* issue that just happened in your business that now you need to deal with – it could be a sexual harassment claim, a tip on an employee stealing, or just someone goofing off on the Internet for way too long. Some issues only require the employees involved to get in a room with HR to address, while others require extensive detective work by the good folks in IT. Especially in cases of data theft, fraud, embezzlement, etc., having detail on everything the employee did leading up to the purported "bad deed" will be critical in determining whether something improper occurred or not.

Whether you are the small business owner, head of HR, or in IT, employee investigations are a part of your daily life. In this whitepaper we'll discuss some of the real-world issues businesses face that result in employee investigations, the methodologies used to perform investigations, and then we'll look at why investigating proactively can help.

Let's begin by looking at a few common employee issues that businesses face.

How Employees Cost The Business

Employees are your greatest asset, but they can also prove to be a material liability. There are some you'll need to keep an eye on for a variety of reasons:

No business can afford to waste 6 employees' salaries every year.

Employee Productivity

Employees are the lifeblood of your business. If they're not focused on making your business succeed, they're not making your business succeed. Social Media, online shopping, and personal smartphones (among many, many other online distractions) are taking your employees away from the work they are there to perform.

In a 2012 survey by Salary.com, employees were asked how much time do they spend performing personal tasks online while at work. Figure 1 shows the responses.

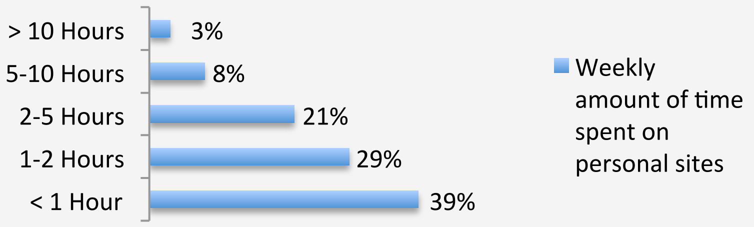


Figure 1: Hours spent weekly on personal websites

I assume your first response to seeing this graph will be "Most people will spend less than an hour. So what's the big deal?" Let's put this into perspective. If you take a 100-person company and apply the time spent to the appropriate percentages (I averaged the amounts of time in each segment, so the 1-2 hours is calculated as 1.5 hours, etc.), you end up with **a total of 226 Hours in a week**! On an annual basis, this is the equivalent amount of time normally put into work-related activities for **6 full-time employees**! No business can afford to waste 6 employees' salaries every year.

Corporate Fraud

The typical company loses 5% of its revenues to fraud annually.

The Association of Certified Fraud Examiners (ACFE) recently reported that the **typical company loses 5% of its revenues to fraud** annually. While 5% doesn't sound like much, how does $140,000? That's the average loss, according to the ACFE, with 20% of losses being **over $1 million**. Let me throw out some additional stats that may shock you:

- **87%** of occupational fraudsters are first-timers
- It takes an average of **18 months** for fraud to be detected
- **49%** of victim organizations never recoup their losses

This is painful stuff. It's real and impactful.

Harassment / Discrimination

The Equal Employment Opportunity Commission (EEOC) released its 2011 findings (the 2012 findings have not been released as of the date of this paper) on sexual harassment and discrimination lawsuits. A few 2011 notables to set the tone:

- There were more than **11,000** Sexual Harassment charges with over **$52M** in damages paid.
- There were more than **32,000** Discrimination charges with over **$98M** in damages paid.

A recent sample of cases highlighted on the EEOC's website mentioned payouts in denominations of "$30,000," "$50,000," and even "$80,000."

Not addressing these types of issues can be costly.

Add onto this one any inappropriate content being watched at work that may be of an illegal or, at very least, offensive nature, which can turn into bigger problems as well.

What Should You Be Watching

The goal in any investigation is, of course, *to find out exactly what the employee in question did.* To accomplish this, you need to perform the normal interviews of involved parties, etc., but you also need to obtain unbiased data that shows what an employee did, said, etc. There are several common data sets you should be aware of from which you should consider reviewing data.

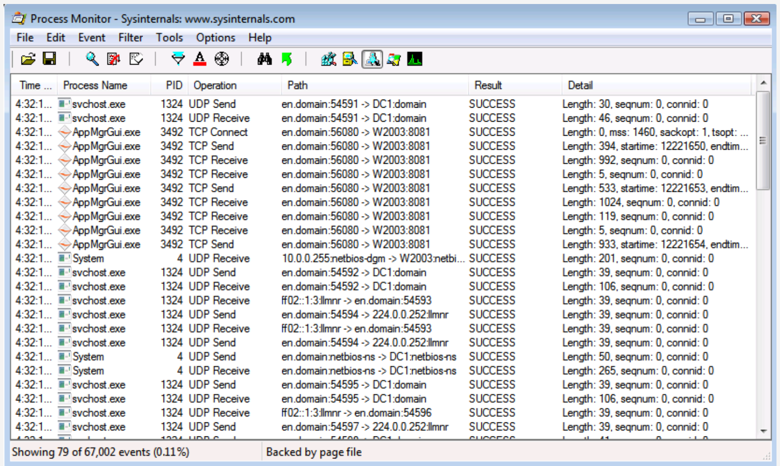
As you read through the remainder of this whitepaper, keep in mind you want to obtain two things as part of your investigation: *proof* and *context*. There will be instances where you can collect enough data to prove an action took place, but it may lack context to discern why it happened.

But is just knowing which apps are in use enough? In most cases, you'd need to see the individual actions within the application to find any offending or incriminating details.

Application Usage

If someone's committing fraud by doctoring the books, the books are most likely in an accounting app. If Facebook is a time-offending website, spending a tremendous amount of time in a web browser is going to be evident.

Microsoft has a free utility, *Process Monitor*, which can provide the answer to the first question, shown in Figure 2.



Time ...	Process Name	PID	Operation	Path	Result	Detail
4:32:1...	svchost.exe	1324	UDP Send	en.domain:54591 -> DC1:domain	SUCCESS	Length: 30, seqnum: 0, connid: 0
4:32:1...	svchost.exe	1324	UDP Receive	en.domain:54591 -> DC1:domain	SUCCESS	Length: 46, seqnum: 0, connid: 0
4:32:1...	AppMgrGui.exe	3492	TCP Connect	en.domain:56080 -> W2003:8081	SUCCESS	Length: 0, mss: 1460, sackopt: 1, tsopt: ...
4:32:1...	AppMgrGui.exe	3492	TCP Send	en.domain:56080 -> W2003:8081	SUCCESS	Length: 394, startime: 12221650, endtim...
4:32:1...	AppMgrGui.exe	3492	TCP Receive	en.domain:56080 -> W2003:8081	SUCCESS	Length: 992, seqnum: 0, connid: 0
4:32:1...	AppMgrGui.exe	3492	TCP Receive	en.domain:56080 -> W2003:8081	SUCCESS	Length: 5, seqnum: 0, connid: 0
4:32:1...	AppMgrGui.exe	3492	TCP Send	en.domain:56080 -> W2003:8081	SUCCESS	Length: 533, startime: 12221653, endtim...
4:32:1...	AppMgrGui.exe	3492	TCP Receive	en.domain:56080 -> W2003:8081	SUCCESS	Length: 1024, seqnum: 0, connid: 0
4:32:1...	AppMgrGui.exe	3492	TCP Receive	en.domain:56080 -> W2003:8081	SUCCESS	Length: 119, seqnum: 0, connid: 0
4:32:1...	AppMgrGui.exe	3492	TCP Receive	en.domain:56080 -> W2003:8081	SUCCESS	Length: 5, seqnum: 0, connid: 0
4:32:1...	AppMgrGui.exe	3492	TCP Send	en.domain:56080 -> W2003:8081	SUCCESS	Length: 933, startime: 12221654, endtim...
4:32:1...	System	4	UDP Receive	10.0.0.255:netbios-dgm -> W2003:netbi...	SUCCESS	Length: 201, seqnum: 0, connid: 0
4:32:1...	svchost.exe	1324	UDP Send	en.domain:54592 -> DC1:domain	SUCCESS	Length: 39, seqnum: 0, connid: 0
4:32:1...	svchost.exe	1324	UDP Receive	en.domain:54592 -> DC1:domain	SUCCESS	Length: 106, seqnum: 0, connid: 0
4:32:1...	svchost.exe	1324	UDP Receive	ff02::1:3:llmnr -> en.domain:54593	SUCCESS	Length: 39, seqnum: 0, connid: 0
4:32:1...	svchost.exe	1324	UDP Send	en.domain:54594 -> 224.0.0.252:llmnr	SUCCESS	Length: 39, seqnum: 0, connid: 0
4:32:1...	svchost.exe	1324	UDP Receive	ff02::1:3:llmnr -> en.domain:54593	SUCCESS	Length: 39, seqnum: 0, connid: 0
4:32:1...	svchost.exe	1324	UDP Send	en.domain:54594 -> 224.0.0.252:llmnr	SUCCESS	Length: 39, seqnum: 0, connid: 0
4:32:1...	System	4	UDP Send	en.domain:netbios-ns -> DC1:netbios-ns	SUCCESS	Length: 50, seqnum: 0, connid: 0
4:32:1...	System	4	UDP Receive	en.domain:netbios-ns -> DC1:netbios-ns	SUCCESS	Length: 265, seqnum: 0, connid: 0
4:32:1...	svchost.exe	1324	UDP Send	en.domain:54595 -> DC1:domain	SUCCESS	Length: 39, seqnum: 0, connid: 0
4:32:1...	svchost.exe	1324	UDP Receive	en.domain:54595 -> DC1:domain	SUCCESS	Length: 106, seqnum: 0, connid: 0
4:32:1...	svchost.exe	1324	UDP Receive	ff02::1:3:llmnr -> en.domain:54596	SUCCESS	Length: 39, seqnum: 0, connid: 0
4:32:1...	svchost.exe	1324	UDP Send	en.domain:54597 -> 224.0.0.252:llmnr	SUCCESS	Length: 39, seqnum: 0, connid: 0

Showing 79 of 67,002 events (0.11%) | Backed by page file

Figure 2: Process Monitor

This can be run on an employee's machine and create a log of every application they run. Keep in mind, you'll be left with a very long log file to sort through and make sense of.

But is it enough to simply know which apps are in use? Process Monitor is only going to show you which apps were in use, but you'll have no insight into what actions were performed. In most cases, you'd need to see the individual actions within the application to find any offending or incriminating details. Some applications provide in-app auditing, keeping track of each action performed – you'd see this commonly if regulatory compliance is a part of life in your industry.

To truly take advantage of application usage information, you'd want to be able to answer the following two questions:

- When was an employee in a particular application?
- What actions were performed?

Communications

If applications represent what an employee *did*, then communications represent what they *said*. Being able to see the unadulterated communications of the employee builds not only a timeline of actions, but also provides a window into the context of why actions were taken.

The most common communications medium today would be corporate email, but communications have taken a leap forward in the past few years where employees are utilizing a wide variety of systems and applications to communicate beyond that of corporate email – webmail, Chat/IM, Skype, Social Media websites all are viable choices (and, in some cases, better choices) to communicate.

Communications have taken a leap forward in the past few years where employees are utilizing a wide variety of systems and applications to communicate beyond that of corporate email.

This makes being able to replay employee communications tough. To add insult to injury, it is important to see both sides of the conversation to ensure you have proper context.

Corporate email platforms like Microsoft Exchange have archiving either built in or available via a third-party provider. Email archives give you the ability to search for sent and received emails, regardless of whether they are deleted on the employee's computer. But beyond that, you are generally out of luck.

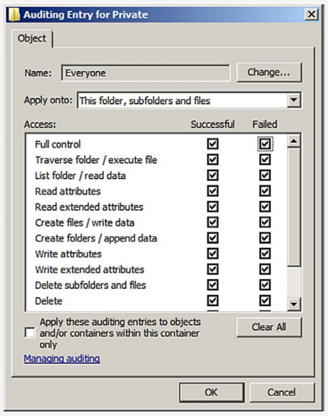
Data Access

Akin to application usage, you need to know what data was accessed by the employee. I've come up with three groups of data to be mindful of:

- In-App data
- File-based data
- Server vs. Local

The in-app data is the most elusive. Very few applications have any kind of reporting as to what was accessed and by whom. But in an investigation, knowing what was accessed helps make your case.

File-based data has been a staple for organizations. Microsoft servers have had File Auditing (shown in Figure 3) built in for years. It needs to be enabled and will only provide auditing on the files and folders configured by IT.



Name: Everyone

Apply onto: This folder, subfolders and files

Access:	Successful	Failed
Full control	☑	☑
Traverse folder / execute file	☑	☑
List folder / read data	☑	☑
Read attributes	☑	☑
Read extended attributes	☑	☑
Create files / write data	☑	☑
Create folders / append data	☑	☑
Write attributes	☑	☑
Write extended attributes	☑	☑
Delete subfolders and files	☑	☑
Delete	☑	☑

☐ Apply these auditing entries to objects and/or containers within this container only

Figure 3: Microsoft File Auditing

Once data has been accessed, what was done with it?

File Auditing needs to be run on each server hosting data and only gives detail on what was done with a file from the perspective of the server. That is, if the file was read from the server, copied to a USB stick and then emailed out via a webmail client, the File Auditing will only show the file was read from the server.

The “server vs. local” data group isn’t exactly unique – it’s really an extension of file-based data, but I mention it because many organizations don’t consider that they need to be aware of data employees are accessing locally as well as from servers. For example, if an employee copies files from a server to the local disk – server-based auditing will record the fact that a file on the server was accessed, but will provide no detail on what was done to it, including the local copy made.

Data Movement

My previous example brings us to this next issue – once data has been accessed, what was done with it? It used to be the only way to copy a file was either to a local storage device (USB, Floppy, CD, etc.) or via email. Today, there’s webmail, Social Media, Cloud-based storage providers, Web transfer protocols and probably a few new ones that neither you nor I are even aware of yet.

This one is as tough as it seems.

Printer Usage

The last data set is the most often overlooked. Printing copies of important documents seems rudimentary, until you realize the printouts can be scanned and the data therein imported into another system. Knowing what was printed and when is important, especially when it comes to issues like fraud and data theft.

Like File Auditing, Microsoft does provide Printer auditing, providing minimal details and certainly no in-page content to show what was printed.

Why Investigations are Difficult

The problem is obvious – there are too many disparate data sets, too many applications, too many pieces of the puzzle to put together. **But that's not really the problem!** Think about it – you're trying to piece together employee actions by watching data and data mediums. That makes no sense. **The problem is you're watching the <u>data</u> and NOT the <u>employee</u>!** To truly get a full picture of an employee's activity you need to be watching… well, the employee's activity.

You're trying to piece together employee actions by watching data and data mediums. That makes no sense. The problem is you're watching the data and NOT the employee!

Since it is ridiculous to conceive of hiring people to watch other people in your organization, what you need is the ability to record an employee's actions on their computer, and the ability to review and replay those actions.

User Activity Monitoring

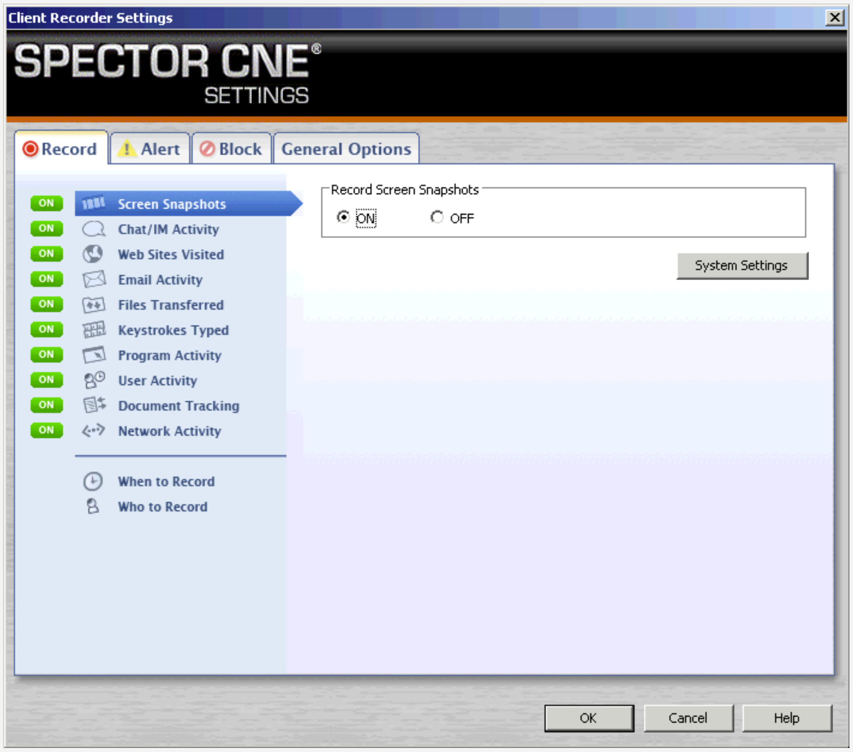
The simple solution is User Activity Monitoring (known as *UAM*) – software that records every action performed on an employee's work computer, organizes that data into meaningful categories, provides the ability to drill down to specific actions, and replays the actions on screen.

Let's work through those four areas of UAM by introducing you to SPECTOR CNE. SPECTOR CNE is SpectorSoft's Employee Investigation software, designed to reduce the time it takes to investigate employees to mere minutes, instead of hours, days, or weeks.

Recording Employee Actions

Think back to all the challenges involved with being able to investigate applications, communications, data access, data movement and printers. By recording every action of a problem employee, you will have a complete record (let me say that again – a *complete record*) of everything the employee did on their computer with actions in sequence, including every application, every chat, every email, every webmail, down to every keystroke. Nothing will be missed.

SPECTOR CNE's recording options, shown in Figure 4, give you the best visual for what you can (and should) collect.



ON Screen Snapshots
ON Chat/IM Activity
ON Web Sites Visited
ON Email Activity
ON Files Transferred
ON Keystrokes Typed
ON Program Activity
ON User Activity
ON Document Tracking
ON Network Activity

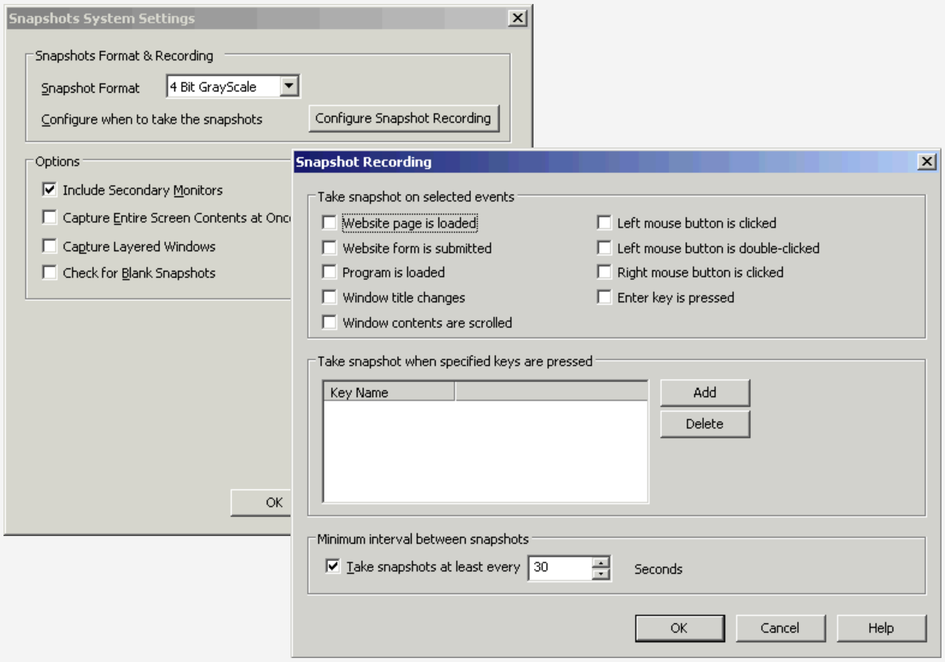
Record Screen Snapshots
● ON ○ OFF

Figure 4: Defining which activity to collect

Everything recorded is centrally stored on a Windows machine (this can be a server or workstation) so you have a secure copy of the recordings for later review and playback, complete with timestamps and watermarks.

Employee Investigations Simplified - Recording
By recording every employee action, you eliminate the need for disparate systems, logs, searches, etc., cutting down the time it takes to both collect and review the data.

One of the most important aspects is the Screen Snapshots. The options, shown in Figure 5, allow you to choose the color, number of screens, frequency and selected events when a screenshot should be taken.



Snapshots Format & Recording

Snapshot Format: 4 Bit GrayScale

Configure when to take the snapshots: Configure Snapshot Recording

Options

☑ Include Secondary Monitors

☐ Capture Entire Screen Contents at Onc

☐ Capture Layered Windows

☐ Check for Blank Snapshots

Take snapshot on selected events

☐ Website page is loaded

☐ Website form is submitted

☐ Program is loaded

☐ Window title changes

☐ Window contents are scrolled

☐ Left mouse button is clicked

☐ Left mouse button is double-clicked

☐ Right mouse button is clicked

☐ Enter key is pressed

Take snapshot when specified keys are pressed

Key Name	

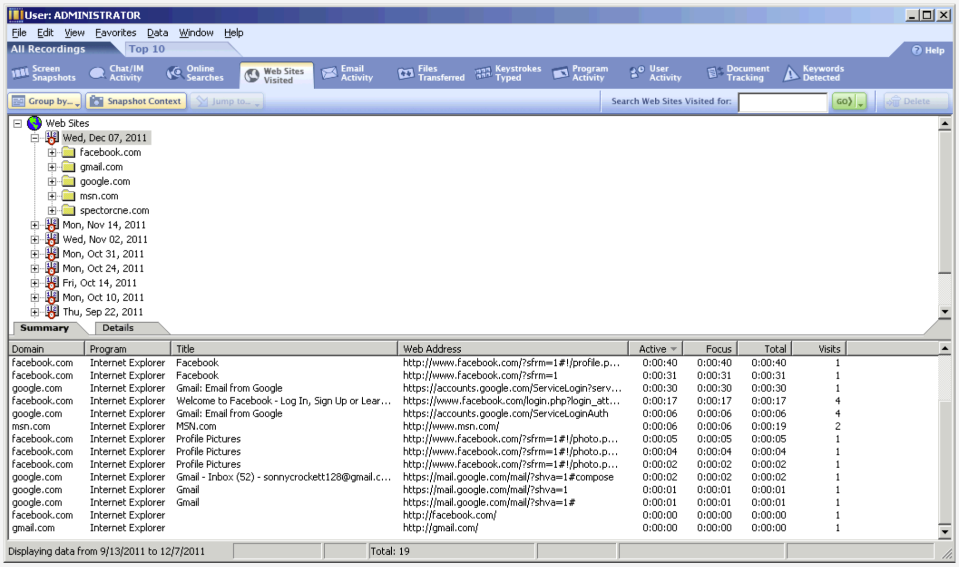
Minimum interval between snapshots

☑ Take snapshots at least every 30 Seconds

Figure 5: Capturing Screen Snapshots

Organizing the Activity

Even when monitoring employee activity, there is still a lot of data to be sorted through. SPECTOR CNE automatically takes the collected activity data and groups it into activity types, as shown in Figure 6.



- Web Sites
  - Wed, Dec 07, 2011
    - facebook.com
    - gmail.com
    - google.com
    - msn.com
    - spectorcne.com
  - Mon, Nov 14, 2011
  - Wed, Nov 02, 2011
  - Mon, Oct 31, 2011
  - Mon, Oct 24, 2011
  - Fri, Oct 14, 2011
  - Mon, Oct 10, 2011
  - Thu, Sep 22, 2011

Domain	Program	Title	Web Address	Active	Focus	Total	Visits
facebook.com	Internet Explorer	Facebook	http://www.facebook.com/?sfrm=1#!/profile.p...	0:00:40	0:00:40	0:00:40	1
facebook.com	Internet Explorer	Facebook	http://www.facebook.com/?sfrm=1	0:00:31	0:00:31	0:00:31	1
google.com	Internet Explorer	Gmail: Email from Google	https://accounts.google.com/ServiceLogin?serv...	0:00:30	0:00:30	0:00:30	1
facebook.com	Internet Explorer	Welcome to Facebook - Log In, Sign Up or Lear...	https://www.facebook.com/login.php?login_att...	0:00:17	0:00:17	0:00:17	4
google.com	Internet Explorer	Gmail: Email from Google	https://accounts.google.com/ServiceLoginAuth	0:00:06	0:00:06	0:00:06	4
msn.com	Internet Explorer	MSN.com	http://www.msn.com/	0:00:06	0:00:06	0:00:19	2
facebook.com	Internet Explorer	Profile Pictures	http://www.facebook.com/?sfrm=1#!/photo.p...	0:00:05	0:00:05	0:00:05	1
facebook.com	Internet Explorer	Profile Pictures	http://www.facebook.com/?sfrm=1#!/photo.p...	0:00:04	0:00:04	0:00:04	1
facebook.com	Internet Explorer	Profile Pictures	http://www.facebook.com/?sfrm=1#!/photo.p...	0:00:02	0:00:02	0:00:02	1
google.com	Internet Explorer	Gmail - Inbox (52) - sonnycrockett128@gmail.c...	https://mail.google.com/mail/?shva=1#compose	0:00:02	0:00:02	0:00:02	1
google.com	Internet Explorer	Gmail	https://mail.google.com/mail/?shva=1	0:00:01	0:00:01	0:00:01	1
google.com	Internet Explorer	Gmail	https://mail.google.com/mail/?shva=1#	0:00:01	0:00:01	0:00:01	1
facebook.com	Internet Explorer		http://facebook.com/	0:00:00	0:00:00	0:00:00	1
gmail.com	Internet Explorer		http://gmail.com/	0:00:00	0:00:00	0:00:00	1

Displaying data from 9/13/2011 to 12/7/2011 Total: 19

Figure 6: View activity easily with SPECTOR CNE

Activity types include:

- Chat/IM Activity
- Online Searches
- Websites Visited
- Email Activity
- Files Transferred
- Keystrokes Typed
- Program Activity
- User Activity
- Document Tracking
- Keywords Detected

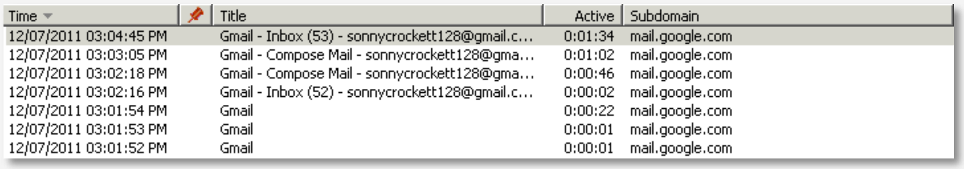
SPECTOR CNE also employs a “Top 10” tab to show the most frequently occurring activities.

Employee Investigations Simplified - Categorizing
By categorizing every employee action, investigators can hone in on the offending type of action quickly.

Activity Drill Down

You’re not looking for general activity; you’re looking for a very specific action – Did the employee email the customer list? Was an inappropriate comment made over IM? How much time was spent on Facebook this week? You need to find that one action – and quickly.

SPECTOR CNE uses both turnkey and custom groupings to expose the detail – down to the keystroke – of what happened. Figure 7 shows detail on emails being sent out through gmail.



Time	📌	Title	Active	Subdomain
12/07/2011 03:04:45 PM		Gmail - Inbox (53) - sonnycrockett128@gmail.c...	0:01:34	mail.google.com
12/07/2011 03:03:05 PM		Gmail - Compose Mail - sonnycrockett128@gma...	0:01:02	mail.google.com
12/07/2011 03:02:18 PM		Gmail - Compose Mail - sonnycrockett128@gma...	0:00:46	mail.google.com
12/07/2011 03:02:16 PM		Gmail - Inbox (52) - sonnycrockett128@gmail.c...	0:00:02	mail.google.com
12/07/2011 03:01:54 PM		Gmail	0:00:22	mail.google.com
12/07/2011 03:01:53 PM		Gmail	0:00:01	mail.google.com
12/07/2011 03:01:52 PM		Gmail	0:00:01	mail.google.com

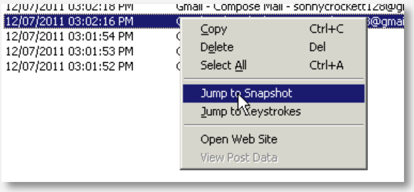
Figure 7: Uncovering the details

Employee Investigations Simplified – Drill Down
Because every employee action is captured, investigators only need a single solution to find the answers in a matter of minutes.

Replaying Activity

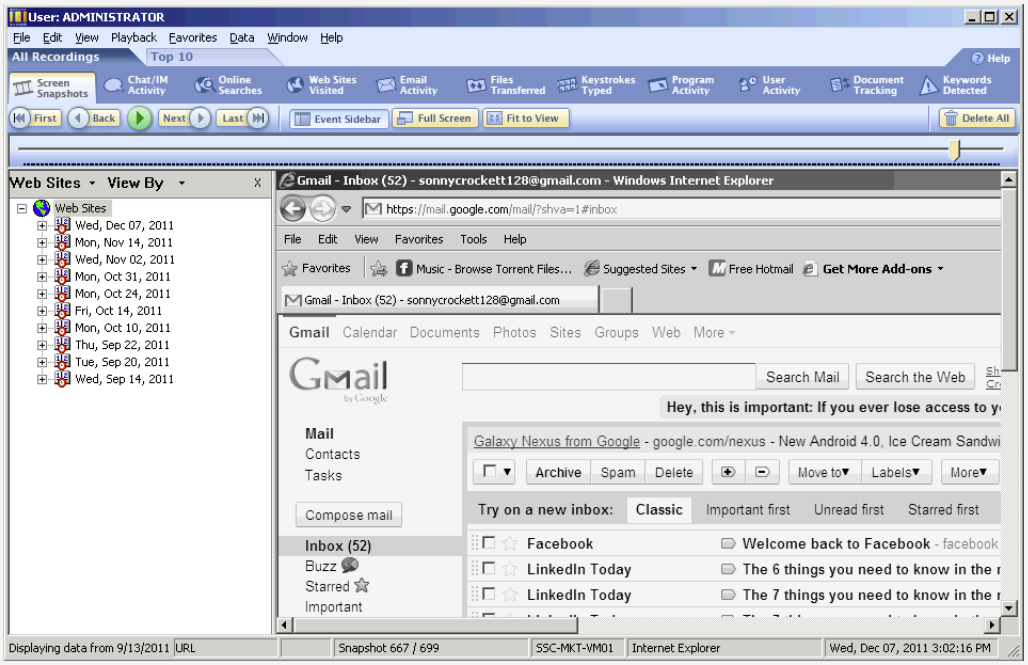
This is where it gets good. With any other investigative method, you can (at best) collect data that infers a user performed a certain action (for example, web logs that show they went to a certain website, but doesn’t specifically show what they did on the page). By taking Screen Snapshots and playing them back, you can watch the employee as if you were standing over their shoulder.

SPECTOR CNE makes it simple to view the screen snapshot of that action you drilled down to so you can complete the story. By right-clicking any action, as shown in Figure 8, you can jump to the snapshot that corresponds with an action, shown in Figure 9.



12/07/2011 03:02:18 PM Gmail - Compose Mail - sonnycrockett128@gmail
12/07/2011 03:02:16 PM
12/07/2011 03:01:54 PM
12/07/2011 03:01:53 PM
12/07/2011 03:01:52 PM

Figure 8: Jumping from Action to Snapshot



Web Sites
Wed, Dec 07, 2011
Mon, Nov 14, 2011
Wed, Nov 02, 2011
Mon, Oct 31, 2011
Mon, Oct 24, 2011
Fri, Oct 14, 2011
Mon, Oct 10, 2011
Thu, Sep 22, 2011
Tue, Sep 20, 2011
Wed, Sep 14, 2011

Hey, this is important: If you ever lose access to y

Galaxy Nexus from Google - google.com/nexus - New Android 4.0, Ice Cream Sandwi

Facebook — Welcome back to Facebook - facebook
LinkedIn Today — The 6 things you need to know in the r
LinkedIn Today — The 7 things you need to know in the r

Displaying data from 9/13/2011 | URL | Snapshot 667 / 699 | SSC-MKT-VM01 | Internet Explorer | Wed, Dec 07, 2011 3:02:16 PM

Figure 9: Viewing Screen Snapshots

Control buttons to Play, Pause, move Next and Back are found to view the employee actions over time. You can also use the screen snapshots to navigate to an action in question, like any other data set in SPECTOR CNE.

Employee Investigations Simplified – Replaying Activity

Being able to replay employee activities is a significant step above alternatives. By replaying the employee's screen, you not only obtain *proof* that something occurred, but you also get *context*. By seeing what they did before and afterwards, you have the benefit of seeing intent and even motives.

Conclusion

The need for employee investigation is clear. The challenge is how to perform and employee investigation in a way that is cost-effective, fast, and easy. SPECTOR CNE provides a unique solution to capture everything an employee does, giving you the information you need to take action.

SPECTOR CNE RESOURCES

Pricing
SPECTOR CNE is priced per-seat, starting at $405 for 3 seats to monitor your Windows-based clients.

For more information or to order a larger quantity, contact SpectorSoft and ask to speak to a sales consultant for your business needs.
☎ (888) 598-2788
💻 www.SPECTORCNE.com

About the Author

Nick Cavalancia, MCSE/MCT/MCNE/MCNI, is SpectorSoft's VP of Marketing where he assists in driving innovation and the evangelism of SpectorSoft solutions. He has over 18 years of enterprise IT experience and is an accomplished consultant, trainer, speaker, columnist and author. He has authored, co-authored and contributed to over a dozen books on Windows, Active Directory, Exchange and other Microsoft technologies.