

# ClubHACKMag

Issue 5 | Jun 2010  
[www.chmag.in](http://www.chmag.in)

1st Indian "HACKING" Magazine



**TechGyan** DLP | **LegalGyan** SOURCE CODE THEFT AND THE LAW |  
**ToolGyan** OPEN DLP | **Mom's Guide** NEW EMAIL SCAM |

It's time to close your leaking taps!!! In this issue we will be covering the complex issue of data leakage and ways to prevent it . Since the issue of data loss is very complicated , an open source solution must be able to address this and that's the reason we love open source community so much. We will be having a look on the new tool OpenDLP to keep an eye on your data.

Apart from DLP, which we have discussed in our techgyan & toolgyan, we also have our legal gyan of this month giving information about law pertaining to data theft & a real life case which happened in India. Let's see how the court reacted to this case. In our other regular sections , Mom's guide is looking at yet another email scam and command line gyan will give shortcuts of finding text/string in bunch of files in an

easy

way.

And Yeh! good news for all you Geeks,Nerds and Hackers. Now you can send in your articles to us and guess what we will publish it in your very own CHmag. Send in your articles to [info@chmag.in](mailto:info@chmag.in)



**Pankit Thakkar**

## ClubHACKMag

Issue 5, June 2010.

### Team CHmag

Rohit Srivastwa  
[rohit@clubhack.com](mailto:rohit@clubhack.com)

Aarja Bhattacharyya  
[aarja@chmag.in](mailto:aarja@chmag.in)

Abhijeet R Patil  
[abhijeet@chmag.in](mailto:abhijeet@chmag.in)

Abhishek Nagar  
[abhishek@chmag.in](mailto:abhishek@chmag.in)

Deepranjan S More  
[deepranjan@chmag.in](mailto:deepranjan@chmag.in)

Pankit Thakkar  
[pankit@chmag.in](mailto:pankit@chmag.in)

Varun V Hirve  
[varun@chmag.in](mailto:varun@chmag.in)

[www.chmag.in](http://www.chmag.in)  
[info@chmag.in](mailto:info@chmag.in)

CONTENTS	Pg 03	<b>TechGyan</b> Data Loss Prevention
	Pg 09	<b>Mom'sGuide</b> Robbed in London: New email scam
	Pg 12	<b>LegalGyan</b> Source Code Theft & the Law
	Pg 18	<b>SpecialFeature</b> CNIP2010 – An Indo UK workshop on Critical National Infrastructure Protection.
	Pg 23	<b>ToolGyan</b> Open DLP
	Pg 28	<b>Command LineGyan</b> Counting & Matching Text in Files



## Data Loss Prevention

---

### Introduction

Information=Money! Information can be anything –financial statements, health records of patients, source codes, intellectual property (IP), trade secrets, design specifications, price lists - anything from which an organization generates profits. Information is one of the business's most important assets.

Business requires accessing information from anywhere, anytime and on any device. This desire for information to be 'free' leads

to many security and management related challenges.

Organizations are moving from securing IT infrastructure to securing Information. While a great deal of attention has been given to protecting electronic assets from outside threats – from IPS to Firewalls to Vulnerability management – organizations are now turning their attention to an equally dangerous situation: the problem of data loss from inside.

### Data Loss Problem

You may have got a complete arsenal of hardware and software, encryption and firewalls, IDS and IPS, to prevent any hacker, virus, malware or spyware from penetrating your defenses. From the outside you are invincible.

Inside is a different story!

Inside, A Blackberry can be as dangerous as an internal spy. Your email server may become a superhighway for sending classified data to the outside world. An HTTP link can be a pipeline to the competition.

The issue of data loss covers everything from confidential information about one customer being exposed, to thousands of source code files for a company's product being sent to a competitor. Whether deliberate or Accidental, data loss occurs any time. Employees, consultants, or other insiders release sensitive data about customers, finances, intellectual property, or other confidential information (in violation of company policies and regulatory requirements).

According to a survey, Employee error is now the fourth largest security concern in the enterprise – behind malware, spyware and spam. With all the avenues available to employees today to electronically expose sensitive data, the scope of the data loss problem is an order of magnitude greater than threat protection from outsiders.

### Sources of Data Leakage

There are many ways through which confidential data or proprietary secrets can leave an organization via the internet: -

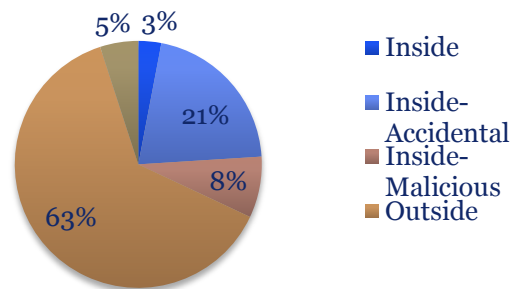
- E-mail
- HTTP (message boards, blogs and other websites)
- Instant Messaging
- Peer-to-peer sites and sessions
- FTP

Flash drives, USB Devices, mp3 players, cell phones, etc. are the most common electronic devices used to leak sensitive data.

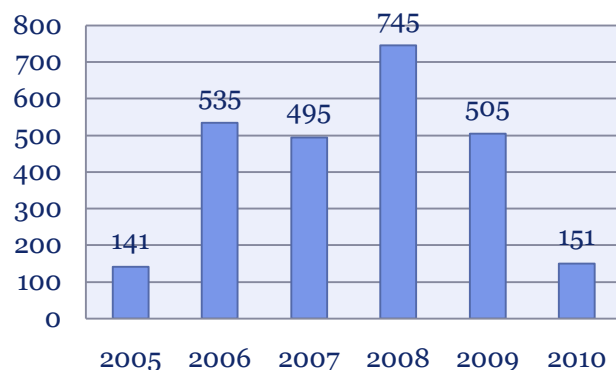
### Data Loss Statistics

The charts below are provided in "as-is" format based on the current database maintained by Open Security Foundation and [DataLossDB.org](http://DataLossDB.org).

**Incidents by Vectors - All Time**



**Incidents Over Time**



## Data Loss Prevention

Data Loss Prevention (DLP) is a system/process for identifying, monitoring and protecting sensitive data on information in an organization according to policies. Policies can vary from organization to organization, but the focus is on preventing sensitive data from leaking out of the organization and identifying people or places that should not have access to certain data or information.

DLP is also referred to as :- Information Leak Prevention (ILP), Information Leak Detection and Prevention (ILDP), Data Leak Prevention, Content Monitoring and Filtering (CMF), Information Protection and Control (IPC), Extrusion Prevention System, etc.

## Sensitive Data and DLP Solution

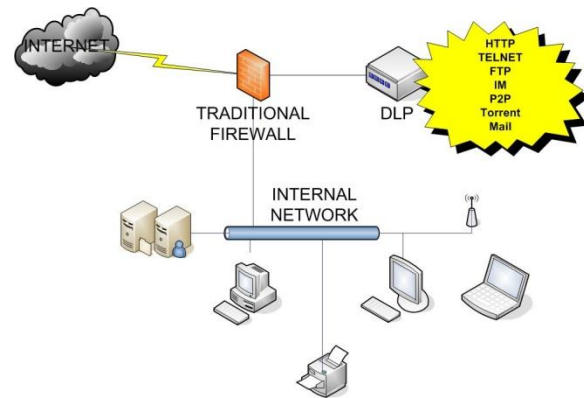
### Data in Motion

This feature of the DLP solution applies to all data on wire. It is basically any data that is moving through the network to the outside via the internet.

Currently, there are various protocols supported and HTTP, FRP, IM, P2P, SMTP to name a few.

As shown below, all traffic leaving internal network via any of the common channels above will be mirrored to DLP for inspection.

See the following example of placement of this device:-



This provides visibility into a large number of violations, For example, if a sensitive file was transferred using FTP, there are several things that will bring to light. FTP is a protocol that uses cleat text. Transmitting sensitive files in clear text becomes a concern. This leads to the question if this file should even be leaving the company. Also we will need to verify if the parties involved are authorized to view and transmit data. Most of this applies not just to FTP, but to any communication mentioned above.

### Data at Rest

This feature refers to any data that resides in file systems, databases and other storage methods. Primary use of this feature is for finding sensitive data in the places where it should not be i.e on corporate network, employee's laptops, backup media, etc. Once it is found, data can be erased, moved to a secured location or protected with access privileges.

This uses the existing policy to look for any sensitive data. Discovery scanning can be used to fingerprint data to indentify unstructured data elsewhere.

### Data at Endpoints

Data at Endpoints constitutes agents that run on end-servers, user laptops or desktops, keeping watch on all activities

related to data. They typically monitor and prevent any data leaving via removable devices such as floppies, CDs, USB devices, external devices, mp3 players etc.

Due to its agent based approach, it really has not been a favorable solution among customers. However it does provide a great deal of protection against erasing data via removable devices.

## Best Practices to Prevent Data Loss

### Best Practice 1:-

#### *Identify and Prioritize Your Most Vulnerable Risk Points*

Unwanted internal and external disclosure of Non-Public Information (financial, business, HR, legal, and regulatory data), Personally Identifiable Information (social security numbers, credit card information, personal health data), and Intellectual Property (patents, trademarks, design plans) can occur at many different points throughout your network. This is why a comprehensive DLP solution ultimately has to protect all potential risk points in your organization.

While end-to-end protection of all vulnerable sites is the ultimate goal for a DLP solution, in reality, it makes far more tactical and financial sense to begin by protecting the data — as well as the mechanisms used to move this data — that represents the most danger to your enterprise. As the most frequently accessed and used electronic application in all companies, email is, without question, the most susceptible data loss risk point for most enterprises. With literally every employee in a typical organization sending

and receiving more than 100 messages every day, it's an obvious vessel for sensitive and confidential information to go where it shouldn't. Adding to this security threat is the fact that email can originate from several different locations, many with gaping security holes, including desktops, mobile devices, public computers, Web-based corporate email, and disconnected laptops.

Not far behind email propagated enterprise risks are via removable storage devices — USB keys, iPods, CD/DVD burners, and disconnected laptops — that can hold hundreds of megabytes of data. Control-free Web activity also represents a Pandora's Box of data loss opportunities, particularly due to popular social networking and file-sharing tools such as instant and third-party messaging, Webmail, internet forums, blogs, and wikis.

Additional enterprise vulnerabilities that need to be addressed include scanning file systems, repositories, document management systems, mail archives for sensitive and confidential data, as well as communication protocols such as FTP, general SMTP, and HTTP.

### Best Practice 2:-

#### *Ensure Effective, Comprehensive Coverage*

A DLP solution must be able to effectively and comprehensively detect attempted policy violations. This includes:

- Multi-protocol monitoring and prevention
- Content-level analysis of all major file and attachment types
- Selective blocking and/or quarantining of messages
- Automatic enforcement of corporate encryption policies

Additionally, companies need to ensure that compliance and policy officers have the capability to create policies by user. Different people have different roles and responsibilities; having a DLP solution that recognizes this and helps enforce appropriate, user-level policies is very important.

If the chosen DLP solution cannot perform comprehensive and accurate content analysis, you won't be able to find and resolve true violations among a mass of false positives. As a result, this ineffective detection system will prevent you from proactively blocking potential data loss violations with confidence, since so many of those flagged actions will be legitimate business activities.

### **Best Practice 3:-**

#### *Insist on Proven and Pre-Built Policies*

An extensive set of effective policies — one that employs full and accurate analysis to provide the right response for any given event — is the foundation of any DLP solution. While it is critical to be able to quickly and easily create and deploy policies, it is just as important that the policies you employ effectively capture your company's best practices and business rules.

Your DLP solution should draw on a complete set of customizable, prebuilt, and tested policies that can address an array of security and compliance issues or target a particular area of risk with pinpoint precision. Most must be 100% ready for immediate deployment across all critical risk points, including e-mail, Web, and Instant Messaging. Some may require customer specific configuration to ensure optimum operation in a particular environment. With either approach, the time and effort required to design,

prioritize, develop, and deploy your DLP policies will be dramatically reduced.

### **Best Practice 4:-**

#### *Protect More than Just Confidential and Sensitive Data*

In addition to preventing information, security breaches of Personally Indefinable Information (credit card information, health record), Intellectual Property (patents, trademarks, designs) and Non-Public Information (financial, business, HR, legal data), your DLP solution should also lessen all risks created by unsafe or noncompliant behavior conducted electronically. This broad range of activity can include unsuitable and offensive employee behavior, communication not in compliance with various regulatory and jurisdictional requirements, behavior that could compromise legal activity and strategy, uncontrolled financial transactions, and inappropriate handling of customer complaints.

An effective Data Loss Prevention solution can and should be used to resolve a wide range of information risk issues beyond guarding sensitive and confidential information. Most companies start by addressing DLP related concerns first, and then expand protection to other areas, such as information misuse.

### **Best Practice 5:-**

#### *Respond Appropriately to Each incident*

Once an event has been determined to be a violation, your DLP solution should respond in real time with the appropriate action such as blocking, quarantining, warning, encrypting, or informing, and then provide suitable steps for immediate remediation. Each response should be gauged specifically

to the type and severity of the violation — in particular, by considering who is involved.

Other appropriate responses include redirecting a message or a user to an informative webpage on company security policy, providing procedural support to complete the task at hand, classifying the relevant message or file, updating an incident dashboard, and silently capturing problematic activity. In addition, you should be able to move, copy, delete, or tag all files at rest.

To ensure that breaches are addressed wherever they occur, responses must originate at all potential risk points, including desktop, message server, network boundary, files repositories, and upon import and analysis of historical events.

### Best Practice 6:-

#### *Training and Awareness*

It is important for an effective DLP solution to interact with the organizations employees so that they have a strong understanding why certain activities are inappropriate and could be harmful for the organization. Not all violations are conducted with harmful intent. An employee may want to work at home and e-mail sensitive data to their personal, less secure public accounts. Although the intent may be good, the action is not. Ongoing education will help reinforce correct behavior and provide the employee with guidance on how to correctly handle sensitive data.

When companies educate and highlight the dangers of data loss, violations are reduced dramatically. Over time, as the employees become more familiar with corporate policy, overall security awareness practices increase throughout the company.

### Conclusion

DLP is a serious issue for companies, as the number for incidents and the cost to those experiencing them continues to increase. Implementing a compressive DLP program is essential for today's working environment.. Whether it's malicious attempt, or an inadvertent mistake, data loss can diminish a company's brand, reduce shareholder value, and damage the company's goodwill and reputation. In today's business environment, the increase in the volume of data is such that this is a challenge to efficiently manage new existing data. Nevertheless, it is a problem that all organizations need to address.



**Abhijeet Patil**  
abhijeet@chmag.in



## Mom's GUIDE



## Robbed in London: New email scam

Recently I came across a new email scam strategy. In this you will get a mail from your friend's email address, saying that your friend went to some place (London preferably) for vacation and got mugged in the hotel. She lost everything except the passport. Now she needs money to pay the hotel bills and come back to her place. So she requests you to loan her some money (mostly around \$1000) which she promises to pay back once she will be back. Also the money has to be transferred through Western Union Money Transfer. Following is the exact content:

"From: YOUR FRIEND  
Sent: Wednesday, March 03, 2010 11:15 PM  
Subject: Sad News!!!

I'm writing this with tears in my eyes, my family and I came down here to London, England for a short vacation unfortunately we were mugged at the park of the hotel where we stayed, All cash, credit card and cell were stolen off us but luckily for us we still have our passports with us. We've been to the embassy and the Police here but they're not helping issues at all and our flight leaves in less than 3hrs from now but we're having problems settling the hotel bills and the hotel manager won't let us leave until we settle the bills.  
Am freaked out at the moment..."

Seems like they first hack the email account, change the password so that the victim won't be able to access her account. Then send mails to the people in the contact list. Though it's new to me but seems similar stuff already happened through Facebook. Details of the earlier incidents were reported at <http://wcbstv.com/technology/facebook.london.phishing.2.1148617.html>. Also a funny

discussion of the hacker and a person to whom the hacker was seeking help after compromising a facebook account could be found at

<http://www.businessinsider.com/2009/1/nigerian-scammers-still-roosting-on-facebook>.

But this time in case of my friend it was not facebook but msn. So seems like they are now spreading their access over the accounts. Now once you are victimized what should you do???

Well, following are few things you could do to prevent your friends from falling prey of the trap:

- Firstly make sure you have a strong password for your account containing upper case and lowercase letters, digits and at least one special symbol like #, \$, & etc.
- Better to change your password every 3 months or so.

These will reduce the probabilities of being hacked. But still there is a chance and if that happens and your friends start getting scam mails from your account, do the following:

1. Try to login to the compromised account. If you are lucky enough to get into the account change the password immediately. You can also try "Forgot Password" option if that is working.
2. If you could login to the account, mail all your contact stating that your this account was hacked and do not reply to any mail from this account.
3. Also if you have any other accounts (facebook, orkut, linkedin etc),

please update your status with the same information so that others will be informed about the same.

4. If you have any other email account, log in to that and inform everybody in your contact. (Luckily you might have the same set of contacts that the compromised account has.)
5. If you are using the same password in your other accounts change it immediately.
6. Also you can try reporting the incident to your email service provider and request them to block or reset the account and give it back to you. This process varies for different email service providers.
  - a. For Gmail - <http://www.labnol.org/inter-net/email/google-account-hacked-gmail-password-change/1947/>
  - b. For hotmail/msn - [http://help.live.com/Help.aspx?market=en-US&project=LiveIDv1&querytype=topic&query=Accountv1\\_TROU\\_UnauthorizedAccess.htm](http://help.live.com/Help.aspx?market=en-US&project=LiveIDv1&querytype=topic&query=Accountv1_TROU_UnauthorizedAccess.htm)
  - c. For yahoo - <http://blog.taragana.com/index.php/archive/best-way-to-recover-your-hacked-yahoo-account/>.
7. If you want to go further, you can contact the corresponding law and enforcement agency who deals with

cyber crime, for further investigation.

8. In case of investigation, email headers of the scam mails could be useful as they could give the IP addresses of the hacker which could lead to her location. So better ask your friends who got the mails to keep the mails/capture the email header and store for further investigation.
9. Also using ReadNotify you can trace the hacker and give that information to the law and enforcement agency. You can get it from - <http://www.readnotify.com/>
10. Last but not the least; it could be possible that the hacker was using some sort of Trojan or key-logger in your computer to get the account information. So scan your computer by antivirus/anti-Trojan software to ensure that your machine is clean.

Also keep yourself always updated with the knowledge of various scams and let others know.



### Tamaghna Basu

[tamahawk-techguru.blogspot.com](http://tamahawk-techguru.blogspot.com)

<http://twitter.com/titanlambda>

Tamaghna has worked on various technologies like java, .net, ruby and various domains including networking and platforms as well.

Has done certifications like RHCE, CEH, ECSA, "Diploma in Cyber Law" and "Cyber Crime Investigation". He He has also attended "Sec 504: Hacker Techniques, Exploits and Incident Handling" training from SANS institute



**Modus Operandi:** If the suspect is an employee of the victim, he would usually

## Source Code Theft & the Law

Computer source code is the most important asset of software companies. Simply put, source code is the programming instructions that are compiled into the executable files that are sold by software development companies.

As is expected, most source code thefts take place in software companies. Some cases are also reported in banks, manufacturing companies and other organizations that get original software developed for their use.

### Scenario 1:

The suspect (usually an employee of the victim) steals the source code and sells it to a business rival of the victim.

have direct or indirect access to the source code. He would steal a copy of the source code and hide it using a virtual or physical storage device. If the suspect is not an employee of the victim, he would hack into the victim's servers to steal the source code. Or he would use social engineering to get unauthorised access to the code. He would then contact potential buyers to make the sale.

**Usual motives:** Illegal financial gain.

### Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43, 65 & 66 of the <i>Information Technology Act</i> and section 63 of <i>Copyright Act</i>	Sections 43, 65, 66 & 66B of the <i>Information Technology Act</i> and section 63 of <i>Copyright Act</i>

## Scenario 2:

The suspect (usually an employee of the victim) steals the source code and uses it as a base to make and sell his own version of the software.

**Modus Operandi:** If the suspect is an employee of the victim, he would usually have direct or indirect access to the source code. He would steal a copy of the source code and hide it using a virtual or physical storage device. If the suspect is not an employee of the victim, he would hack into the victim's servers to steal the source code. Or he would use social engineering to get unauthorised access to the code.

He would then modify the source code (either himself or in association with other programmers) and launch his own software.

**Usual motives:** Illegal financial gain.

### Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43, 65 & 66 of the <i>Information Technology Act</i> and section 63 of <i>Copyright Act</i>	Sections 43, 65, 66 & 66B of the <i>Information Technology Act</i> and section 63 of <i>Copyright Act</i>

Section 65 of the Information Technology Act is titled "Tampering with computer source documents" and is the most important legal provisions relating to source code theft in India.

## 65. Tampering with computer source documents.

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

**Explanation.** - For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

### COMMENTS:

Computer source code is the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form. Computer source code need not only be in the electronic form. It can be printed on paper (e.g. printouts of flowcharts for designing a software application). Let us understand this using some illustrations.

**Illustration:** Pooja has created a simple computer program. When a user double-clicks on the hello.exe file created by Pooja, the following small screen opens up:

Hello World

The hello.exe file created by Pooja is the executable file that she can give to others. The small screen that opens up is the output of the software program written by Pooja. Pooja has created the executable file using the programming language called “C”. Using this programming language, she created the following lines of code:

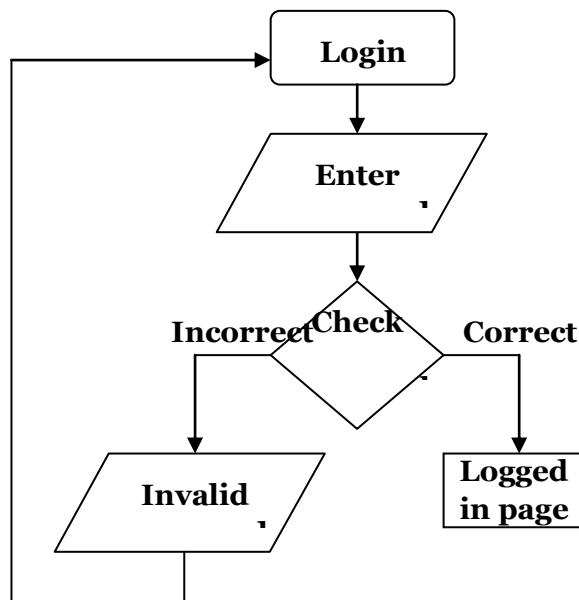
```
main()
{
    printf("Hello, ");
    printf("World");
}
```

These lines of code are referred to as the source code.

**Illustration:** Noodle Ltd has created software for viewing and creating image files. The programmers who developed this program used the computer-programming language called Visual C++. Using the syntax of these languages, they wrote thousands of lines of code. This code is then compiled into an executable file and given to end-users. All that the end user has to do is double-click on a file (called setup.exe) and the program gets installed on his computer. The lines of code are known as computer source code.

**Illustration:** Pooja is creating a simple website. A registered user of the website would have to enter the correct password to access the content of the website. She creates the following flowchart outlining the

functioning of the authentication process of the website.



She takes a printout of the flowchart to discuss it with her client. The printout is source code.

This section relates to computer source code that is either: (1) required to be kept (e.g. in a cell phone, hard disk, server etc), or (2) required to be maintained by law.

The following acts are prohibited in respect of the source code (1) knowingly concealing or destroying or altering (2) intentionally concealing or destroying or altering (3) knowingly causing another to conceal or destroy or alter (4) intentionally causing another to conceal or destroy or alter. Let us discuss the relevant terms and issues in detail.

*Conceal* simply means “to hide”.

**Illustration:** Pooja has created a software program. The source code files of the program are contained in a folder on Pooja’s laptop. Sameer changes the properties of the folder and makes it a “hidden” folder. Although the source code folder still exists on Pooja’s computer, she can no longer see it. Sameer has concealed the source code.

*Destroy* means “to make useless”, “cause to cease to exist”, “nullify”, “to demolish”, or “reduce to nothing”.

Destroying source code also includes acts that render the source code useless for the purpose for which it had been created.

**Illustration:** Pooja has created a software program. The source code files of the program are contained in a folder on Pooja’s laptop. Sameer deletes the folder. He has destroyed the source code.

**Illustration:** Pooja has created a software program. The source code files of the program are contained in a folder on Pooja’s laptop. Sameer deletes one of the source code files. Now the source code cannot be compiled into the final product. He has destroyed the source code.

**Illustration:** Pooja is designing a software program. She draws out the flowchart depicting the outline of the functioning of the program. Sameer tears up the paper on which she had drawn the flowchart. Sameer has destroyed the source code.

*Alters*, in relation to source code, means “modifies”, “changes”, “makes different” etc. This modification or change could be in respect to size, properties, format, value, utility etc.

**Illustration:** Pooja has created a webpage for her client. The source code of the webpage is in HTML (Hyper Text Markup Language) format. Sameer changes the file from HTML to text format. He has altered the source code.

**CASE LAW:** Syed Asifuddin and Ors. Vs. The State of Andhra Pradesh & Anr. [2005CriLJ4314]

### Summary of the case:

Tata Indicom employees were arrested for manipulation of the electronic 32-bit number (ESN) programmed into cell phones that were exclusively franchised to Reliance Infocomm. The court held that such manipulation amounted to tampering with computer source code as envisaged by section 65 of the Information Technology Act, 2000.

### Background of the case:

Reliance Infocomm launched a scheme under which a cell phone subscriber was given a digital handset worth Rs. 10,500 as well as service bundle for 3 years with an initial payment of Rs. 3350 and monthly outflow of Rs. 600. The subscriber was also provided a 1 year warranty and 3 year insurance on the handset.

The condition was that the handset was technologically locked so that it would only work with the Reliance Infocomm services. If the customer wanted to leave Reliance services, he would have to pay some charges including the true price of the handset. Since the handset was of a high quality, the market response to the scheme was phenomenal.

Unidentified persons contacted Reliance customers with an offer to change to a lower priced Tata Indicom scheme. As part of the deal, their phone would be technologically “unlocked” so that the exclusive Reliance handsets could be used for the Tata Indicom service.

Reliance officials came to know about this “unlocking” by Tata employees and lodged a First Information Report (FIR) under various provisions of the Indian Penal Code, Information Technology Act and the Copyright Act.

The police then raided some offices of Tata Indicom in Andhra Pradesh and arrested a few Tata Teleservices Limited officials for re-programming the Reliance handsets.

These arrested persons approached the High Court requesting the court to quash the FIR on the grounds that their acts did not violate the said legal provisions.

### Issues raised by the Defence:

- (1) Subscribers always had an option to change from one service provider to another.
- (2) The subscriber who wants to change from Tata Indicom always takes his handset, to other service providers to get service connected and to give up Tata services.
- (3) The handsets brought to Tata by Reliance subscribers are capable of accommodating two separate lines and can be activated on principal assignment mobile (NAM 1 or NAM 2). The mere activation of NAM 1 or NAM 2 by Tata in relation to a handset brought to it by a Reliance subscriber does not amount to any crime.
- (4) A telephone handset is neither a computer nor a computer system containing a computer programme.
- (5) There is no law in force which requires the maintenance of "computer source code". Hence section 65 of the Information Technology Act does not apply.

### Findings of the court

- (1) As per section 2 of the Information Technology Act, any electronic, magnetic or optical device used for storage of information received through satellite, microwave or other communication media and the devices which are programmable and capable of retrieving any information by manipulations of electronic, magnetic or optical impulses is a computer which can be used as computer system in a computer network.
- (2) The instructions or programme given to computer in a language known to the computer are not seen by the users of the computer/consumers of computer

functions. This is known as source code in computer parlance.

- (3) A city can be divided into several cells. A person using a phone in one cell will be plugged to the central transmitter of the telecom provider. This central transmitter will receive the signals and then divert them to the relevant phones.
- (4) When the person moves from one cell to another cell in the same city, the system i.e., Mobile Telephone Switching Office (MTSO) automatically transfers signals from tower to tower.
- (5) All cell phone service providers have special codes dedicated to them and these are intended to identify the phone, the phone's owner and the service provider.
- (6) System Identification Code (SID) is a unique 5-digit number that is assigned to each carrier by the licensor. Every cell phone operator is required to obtain SID from the Government of India. SID is programmed into a phone when one purchases a service plan and has the phone activated.
- (7) Electronic Serial Number (ESN) is a unique 32-bit number programmed into the phone when it is manufactured by the instrument manufacturer. ESN is a permanent part of the phone.
- (8) Mobile Identification Number (MIN) is a 10-digit number derived from cell phone number given to a subscriber. MIN is programmed into a phone when one purchases a service plan.
- (9) When the cell phone is switched on, it listens for a SID on the control channel, which is a special frequency used by the phone and base station to talk to one another about things like call set-up and channel changing.
- (10) If the phone cannot find any control channels to listen to, the cell phone displays "no service" message as it is out of range.
- (11) When cell phone receives SID, it compares it to the SID programmed into the phone and if these code numbers match, cell



knows that it is communicating with its home system. Along with the SID, the phone also transmits registration request and MTSO which keeps track of the phone's location in a database, knows which cell phone you are using and gives a ring.

(12) So as to match with the system of the cell phone provider, every cell phone contains a circuit board, which is the brain of the phone. It is a combination of several computer chips programmed to convert analog to digital and digital to analog conversion and translation of the outgoing audio signals and incoming signals.

(13) This is a micro processor similar to the one generally used in the compact disk of a desktop computer. Without the circuit board, cell phone instrument cannot function.

(14) When a Reliance customer opts for its services, the MIN and SID are programmed into the handset. If someone manipulates and alters ESN, handsets which are exclusively used by them become usable by other service providers like TATA Indicom.

kept" (b) "maintained by law for the time being in force".



**Rohas Nagpal**  
rn@asianlaws.org

### Conclusions of the court

(1) A cell phone is a computer as envisaged under the Information Technology Act.

(2) ESN and SID come within the definition of "computer source code" under section 65 of the Information Technology Act.

(3) When ESN is altered, the offence under Section 65 of Information Technology Act is attracted because every service provider has to maintain its own SID code and also give a customer specific number to each instrument used to avail the services provided.

(4) Whether a cell phone operator is maintaining computer source code, is a matter of evidence.

(5) In Section 65 of Information Technology Act the disjunctive word "or" is used in between the two phrases – (a) "when the computer source code is required to be



## Critical National Infrastructure Protection

### CNIP2010 - An Indo UK workshop on Critical National Infrastructure Protection.

*Organized by CDAC Mumbai in association with IIT Gandhinagar & City University London*

On May 14<sup>th</sup> & 15<sup>th</sup>, CDAC Mumbai, IIT Gandhinagar & City University London organized a workshop on information security perspective of Critical National Infrastructure Protection. This workshop was intended to brainstorm and learn more on the information security risk of SCADA systems and other such critical applications of computers. Looking at the rate at which digitalization of our infrastructure is happening and the current state where only a very small part of our critical infrastructure has gone digital, this workshop was organized in a very apt moment. It's necessary for all of us to understand the risk and take proper steps to mitigate during the building phase itself. It would be a shame & disaster if we ignore this aspect at this point of time & build infrastructure for future correction. Due to pre-occupation & time constraint I was not able to speak in this event. So I was chosen to conclude the event with my closing note.

Here's my view of the workshop as an attendee, a closing note speaker as well as a normal tech-savvy citizen

## Day 1 - Tutorials & Product launch

The event started on 14<sup>th</sup> with a tutorial on "Vulnerability and counter measures in Critical Infrastructure SCADA" by CDAC Mumbai & ABB Bangalore. CDAC Mumbai is known to be working on SCADA and related security products where as ABB is an industry leader in manufacturing electrical components, which is a very critical part of the CNI. This tutorial was a real eye opener on the concept and the kind of risk involved at this level.

The second on schedule was product launch by CDAC Mumbai. CDAC had been instrumental in development of some good products in the field of information security and they released 3 products at the event

**1. Disaster Recovery Solution (Revival)** - Revival family (family of 3 solutions) is a hardware based solution which is storage agnostic and can work on almost all popular storage hardware. Based on an Intel ATOM (N270) processor revival family uses iSCSI protocol to talk to 1TB inbuilt storage media. Revival family gives Synchronous, Semi-Synchronous & Optimal DR solution by connecting 1, 2 or multiple revival boxes in local as well as remote locations. CDAC's idea is to provide bundled solution low or zero RTO/RPO solution for critical data installations. To achieve the same, revival also exploits WAN optimization techniques such as compression & recompression.

**My verdict** - Good product & would be really useful if installed and configured properly at critical locations

**2. Intrusion Detection & Prevention System (GYN)** - Guard Your Network or GYN is the name of IDS/IPS created by CDAC which works in inline bridge mode to provide gateway security for networks. GYN1000 claims to provide security against DoS, DDoS, worms, web attacks, email attacks, database attacks, scans, floods, and other anomalies. As per the release note, GYN1000 provides a throughput of 1Gbps with more than 10,00,000 concurrent TCP connections

**My verdict** - I felt like looking at yet another IPS in market unless they prove it to be something very superior. I'd wait to see the product in market with price benefit and/or feature as well as performance.

**3. Secure Two-factor Authentication for Remote Systems (STARS)** - CDAC also launched a java based two factor authentication using text, graphical & tex-o-graphical passwords. A demo of the same was shown where a user can choose authentication solution of his/her choice. STARS give user freedom to opt for any suitable second factor such as smart card, usb token, etc.

**My Verdict** - I feel that this is good as an academic project and might not see a real day light due to the complexity of operation. Users today want an easy solution, not a difficult one. Further development on the same might make it more useful for people, at least for some applications.

## Day 2 - Technical sessions

Second day of the event was scheduled for technical talks. Some of the speakers invited were not able to make it to the event due to some VISA issues. Let's have a look at the technical sessions

### *1. Security and Trust in Group Communication - G Sivakumar, IIT Mumbai*

Prof G Sivakumar gave a very light and simple perspective of trust in communication between peers of groups & projects. The idea was to understand the access levels of different peer members as and when they join or leave the core working group. This kind of communication is very much required in an academic environment when at different times different people join in & leave their working groups

### *2. Cyber Threat to Banking industry - Vishal Salvi, CISO HDFC Bank*

Vishal's talk was targeted towards the banking industry and how banks these days are working day and night to fight fraudsters so as to save customers, themselves as well the money. It was a delight to notice that how banks are taking care to tune systems & process to help user's safety. . In most of the cases we have seen users falling prey to phishing attack by their own ignorance.

### *3. Traitor Tracing - Bimal Roy, ISI Kolkata*

Frankly speaking, this talk was too mathematical and statistical for me to understand. I didn't get a lot from this talk except the fact that many organizations are working seriously to add more and more security & investigative power to the country's pool

### *4. Cyber Security in Network Manager: Power Distribution - Deven Patel, ABB Bangalore*

Deven Patel gave a very nice insight of how power industry works today and what are the steps these companies take to make the system more secure in physical, network & other security aspects. It is very important to understand at this time that every component installed in any critical infrastructure needs to be quality checked with proper control. If a small component used in critical infrastructure is outsourced and not made by these security conscious companies can also create havoc in the infrastructure. For example, the passive insulator being used to separate connectivity, if that is bugged by an adversary during production at an outsourced location can produce inferior product which can cause break down at a very critical stage causing a major loss .

### *5. Small Machines, Big Targets - Sitaram Chamrty, TCS Hyderabad*

Small machines in Sitaram's perspective were the normal desktops & laptops we use today. Indeed they are small in comparison to the SCADA devices but are equal or even bigger targets of attack. Very well pointed by him that in today's scenario, the laptop used by a key position IAS officers is also a part

of Critical Infrastructure for us because the kind of data it holds is very critical. As a normal trend we have seen the same devices being taken home and then used by family members especially kids to play around with. One mistake by these members or even by the officer can cause leakage of data which we have already seen in near past. Sitaram gave a very nice concept of application isolation where as each and every application runs in its own userspace with minimum privileges. He told that he is working on the same and will be releasing the Linux version of the solution soon. We'd really wait to see that it is working and hope to see similar project for windows users.

#### *6. Protecting from phishing attack on ATM - Rajat Moona, IIT Kanpur*

This talk caught attendees in surprise by showing the possibility of fake ATMs. In today's world ATM authenticates users & it's equally important for users to authenticate the ATM machines too. Rajat presented few ideas on which some students on IIT Kanpur were working. These included smart card based & cell phone based authentication where a mutual authentication of both ATM as well as card holder can be done. This kind of solution can also work in remote locations such as villages where connectivity can be an issue. This kind of offline/partially online ATM can be a boon if developed and brought to market.

#### *7. Monitoring & Protection of airwaves from malicious unlicensed radios - Kaustubh Phanse, Airtight Networks, Pune*

Kaustubh presented his views on importance of wireless security where the

minor mistakes and ignorance create havocs in corporate networks. This can also extend to critical installations if users as well as the admins are not alert.

#### *8. Threats to CNI from Mobile attack - Saritha Arunkumar, IBM UK*

Sarita's talk was targeted on mobile application security and its relevance with CNI. From my point of view it was an important talk in information security perspective but not very apt for this platform where most of the discussions were on CNIP. Though a POV was presented on why mobile apps are important in relation with CNIP but somehow I wasn't convinced with that. .

#### *9. The threat on the net - Steven Furnell, Univ of Plymouth, UK*

This was a recorded presentation sent from UK because Steven was unable to travel due to some VISA issues. This talk was again more on an information security perspective but not very closely knit to CNI.

#### *10. SCADA Security - Zia Saquib, CDAC Mumbai*

Last talk of the day was by Executive Director of CDAC Mumbai himself where he again pointed out the need and importance of security in SCADA networks. Knowing the fact that slowly SCADA networks are

getting connected to internet cloud and data is being transmitted over same cloud, it has really become a matter of concern and very strong security measures should be taken to secure our Critical National Infrastructure.

The event concluded by a closing note from my side and vote of thanks from Dhiren Patel, IIT Gandhinagar.

The presentations of the event will be online and can be access from <http://cnip2010.cdacmumbai.in>



**Rohit Srivastwa**  
[rohit@clubhack.com](mailto:rohit@clubhack.com)

---



# Open DLP

## Tool GYAN

## OpenDLP Tool

---

### DLP Tools

Some of the commercial DLP tools available in the market are – CA DLP by CA technologies, Iron Port by Cisco, Data Loss Prevention Products by McAfee.

### OpenDLP

Andrew Gavin released OpenDLP (version 0.1) on 30<sup>th</sup> April 2010 on [code.google.com](http://code.google.com), a free and open source, agent-based, centrally-managed, massively distributable data loss prevention tool.

OpenDLP can simultaneously identify sensitive data at rest on hundreds or thousands of Microsoft Windows systems from a centralized web application. It also helps to implement basic scanning on files lying on your organization's workstations and servers. OpenDLP has two components: a web application and an agent.

### Web Application

- Automatically deploys and starts agents over NetBIOS
- When done, automatically stops, uninstalls, and deletes agents over NetBIOS
- - Pause, resume, and forcefully uninstall agents in an entire scan or on individual systems

- - Concurrently and securely receive results from hundreds or thousands of deployed agents
- Create Perl-compatible regular expressions (PCREs) for finding sensitive data at rest
- Create reusable profiles for scans that include white listing or blacklisting directories and file extensions
- Review findings and identify false positives
- Export results as XML
- Written in Perl with MySQL backend

### Agent

- Runs on Windows 2000 and later versions
- Written in C , no .NET Framework requirements
- Runs as a Windows Service at low priority so users do not see or feel it
- Resumes automatically upon system reboot with no user interaction
- Securely transmits results to web application at user-defined intervals
- Uses PCREs to identify sensitive data inside files
- Performs additional checks on potential credit card numbers to reduce false positives

### Platform Requirement

OpenDLP tool basically runs on Windows 2000 and later versions with no special .NET Framework requirement. It runs as a Windows Service at low priority so users do not see or feel it.

OpenDLP resumes automatically upon system reboot with no user interaction. It uses PCREs to identify sensitive data inside files. The code is written in Perl and stores data into a MySQL database.

OpenDLP securely transmits results to web application at user-defined intervals over two-way-trusted SSL connection. It also uses PCREs (Perl Compatible Regular Expressions) to identify sensitive data inside files. Performs additional checks on potential credit card numbers to reduce false positives.

OpenDLP is released as GPL and all the source code is provided.

As mentioned by Xavier Martin [@xme] on his blog -

<http://blog.rootshell.be/2010/04/30/keep-an-eye-on-your-data-using-opendlp/>

The source code of agent reveals that:

- The agent scans the following storage types: floppy, thumb drive, flash card reader, HDD, flash drive, CD-ROM and RAM disk.
- White/blacklists are available to prevent some files to be scanned.
- Filters based on file extensions.
- libcurl is used to communicate with the server (using SSL)

Once finished, the scan results can be reviewed via the WebGUI and exported as XML for further processing. The search for breaches is performed via Perl regular expressions. The default set of regex is very low but gives a good idea of the “power” of regex. Some regex by Xavier is mentioned in the box below.

## Future Development

Andrew Gavin has already a list of future enhancements.

- Zip support to agent, to read Office 2007 and OpenOffice files.
- Support for Microsoft Word and OpenOffice formats.
- A sniffer mode listening for outbound sensitive data.

```
Credit_Card_Track_1:(\\D|^)\\%?[Bb]\\d{13,19}\\^[-\\|/\\.\\w\\s]{2,26}\\^[0-9][0-9][01][0-9][0-9]{3}
Credit_Card_Track_2:(\\D|^)\\;\\d{13,19}\\=(\\d{3}|)(\\d{4}|\\=)
Credit_Card_Track_Data:[1-9][0-9]{2}\\-[0-9]{2}\\-[0-9]{4}\\^\\d
Mastercard:(\\D|^)5[1-5][0-9]{2}(\\ \\|\\-|)[0-9]{4}(\\ \\|\\-|)[0-9]{4}(\\ \\|\\-|)[0-9]{4}(\\D|$)
Visa:(\\D|^)4[0-9]{3}(\\ \\|\\-|)[0-9]{4}(\\ \\|\\-|)[0-9]{4}(\\ \\|\\-|)[0-9]{4}(\\D|$)
AMEX:(\\D|^)(34|37)[0-9]{2}(\\ \\|\\-|)[0-9]{6}(\\ \\|\\-|)[0-9]{5}(\\D|$)
Diners_Club_1:(\\D|^)30[0-5][0-9](\\ \\|\\-|)[0-9]{6}(\\ \\|\\-|)[0-9]{4}(\\D|$)
Diners_Club_2:(\\D|^)(36|38)[0-9]{2}(\\ \\|\\-|)[0-9]{6}(\\ \\|\\-|)[0-9]{4}(\\D|$)
Discover:(\\D|^)6011(\\ \\|\\-|)[0-9]{4}(\\ \\|\\-|)[0-9]{4}(\\ \\|\\-|)[0-9]{4}(\\D|$)
JCB_1:(\\D|^)3[0-9]{3}(\\ \\|\\-|)[0-9]{4}(\\ \\|\\-|)[0-9]{4}(\\ \\|\\-|)[0-9]{4}(\\D|$)
JCB_2:(\\D|^)(2131|1800)[0-9]{11}(\\D|$)
```



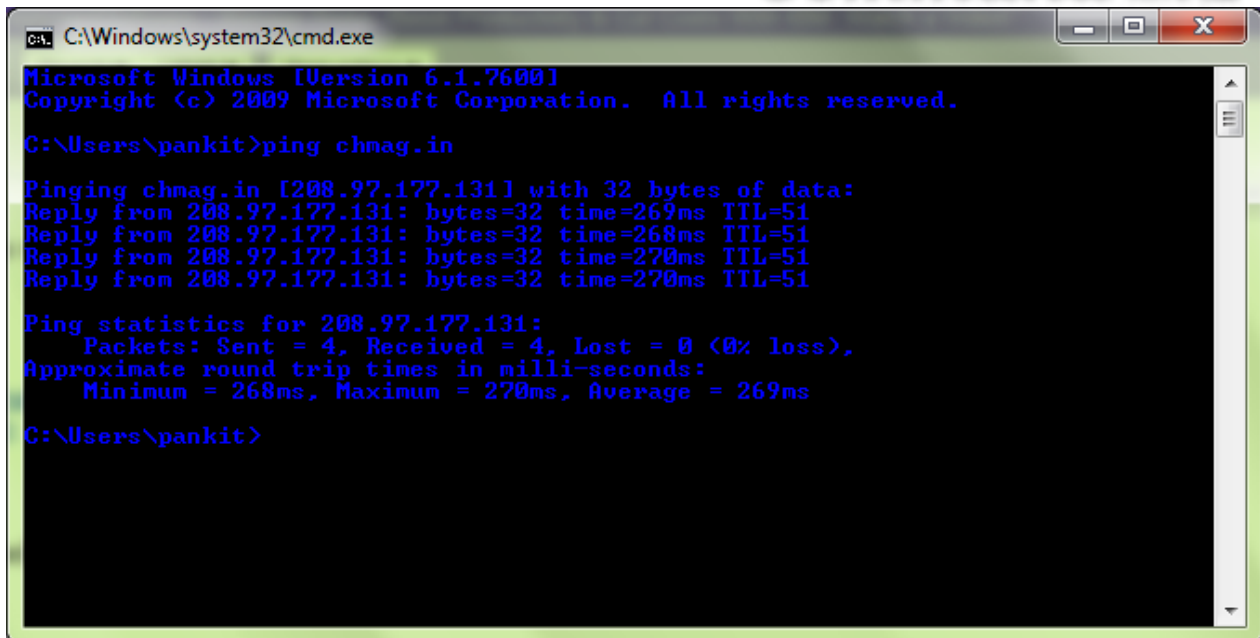
### Applications of OpenDLP Tool:-

- Automatically deploy and start agents over Netbios/SMB
- When done, automatically stop, uninstall, and delete agents over Netbios/SMB
- Pause, resume, and forcefully uninstall agents in an entire scan or on individual systems
- Concurrently and securely receive results from hundreds or thousands of deployed agents over two-way-trusted SSL connection
- Create Perl-compatible regular expressions (PCREs) for finding sensitive data at rest
- Create reusable profiles for scans that include white listing or blacklisting directories and file extensions
- Review findings and identify false positives
- Export results as XML
- Written in Perl with MySQL backend



**Varun Hirve**  
[varun@chmag.in](mailto:varun@chmag.in)

## Command LINE



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\pankit>ping chmag.in

Pinging chmag.in [208.97.177.131] with 32 bytes of data:
Reply from 208.97.177.131: bytes=32 time=269ms TTL=51
Reply from 208.97.177.131: bytes=32 time=268ms TTL=51
Reply from 208.97.177.131: bytes=32 time=270ms TTL=51
Reply from 208.97.177.131: bytes=32 time=270ms TTL=51

Ping statistics for 208.97.177.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 268ms, Maximum = 270ms, Average = 269ms

C:\Users\pankit>
```

## Counting & Matching Text in Files

As we are at finding leaking data, I thought putting something related would be more fun.

In this issue of command line gyan, we'll see how we can find some text in files. Say we are looking for a pattern of text in multiple file. This can also be used in any such DLP to find the leaking data.

### Windows

Here we go with a simple attempt and see how good it is

```
C:\windows> find /c "disk" *.log
```

Output

This switch /c of find command here will search the current directory Driver (C:\windows) for all the .log files where the string "disk" is mentioned. This will print number of occurrences of the substring too.

To further improve it we'll first redirect all the errors to null

```
C:\windows> find /c "disk"
*.log 2>null
```

```
----- SPUPDSUC.LOG: 0
----- STI_TRACE.LOG: 0
----- TABLETOC.LOG: 0
----- TSOC.LOG: 1
----- UPDSPAPI.LOG: 0
----- WGANOTIFY.LOG: 0
----- WIADEBUG.LOG: 0
----- WIASERUC.LOG: 0
----- WINDOWUPDATE.LOG: 0
----- WLAN.LOG: 0
----- WMFDIST11.LOG: 0
----- WMP11.LOG: 0
----- WMSETUP.LOG: 0
----- WMSETUP10.LOG: 0
----- WUDF01000INST.LOG: 0
C:\WINDOWS>
```

Ok, haven't achieved much yet. We are still getting a lot of with "0" occurrences. In a big directory this might not be very useful. So now we'll remove all the lines showing 0 occurrences.

```
C:\windows>find /c "disk" *.log
2>null | find /v ": 0"
```

```
----- SETUPACT.LOG: 2
----- SETUPAPI.LOG: 117

----- TSOC.LOG: 1

C:\WINDOWS>
```

This will now remove all the lines which are showing ": 0"

/v here negates the search string ": 0" & show only those lines which do not have string ": 0"

So far so good, but there are two ugly things in the result

The leading "----" put by find /c command & unnecessary blank lines courtesy to our second find /v of ": 0".

To solve this we'll have to rely on our good old FOR loop.

```
C:\WINDOWS>for /f "delims=--"
%i in ("find /c "disk"
*.log 2>nul | find /v ": 0"
") do @echo %i
```

```
LAN.LOG: 10
MEDCTROC.LOG: 2126
MSCOMPPACKU1.LOG: 109
MSGSOCM.LOG: 1057
MSMQINST.LOG: 1671
NETFXOCM.LOG: 1998
NSM.LOG: 14
NTDICTSETUP.LOG: 2017
OCGEN.LOG: 8959
OCMSN.LOG: 1169
REGOPT.LOG: 37
SESSMGR.SETUP.LOG: 38
SETUPACT.LOG: 2849
SETUPAPI.LOG: 10853
SPUPDSUC.LOG: 470
TABLETOC.LOG: 832
TSOC.LOG: 8765
UPDSPAPI.LOG: 419
WGANOTIFY.LOG: 69
WIADEBUG.LOG: 2
WIASERUC.LOG: 1
WINDOWSUPDATE.LOG: 15727
WLAN.LOG: 10
WMPDIST11.LOG: 446
WMP11.LOG: 312
WMSETUP.LOG: 316
WMSETUP10.LOG: 39
WUDF010000INST.LOG: 206

C:\WINDOWS>
```

I think it's pretty simple from the command that we have removed all unwanted delimiters like "--" & CRFLs. You might wonder how we removed the CRLF (blank lines), basically we didn't parse lines that didn't have "--" in them ☺

So what say now, happy with the output now you can use this output in any report as such.

## Linux

The same can be done in Linux in following way.

If we have to find it in a single file then command below will do the trick.

```
$ grep robot
/var/log/httpd/access/access
.log | wc -l
```

```
[perrier]$ grep robot access.log | wc -l
10
[perrier]$
```

But our objective is to scan a complete directory and search for the string.

So let's create a loop that does the main part of the work, and then piped the output into awk for better reporting.

```
$ for f in *; do echo -n "$f
"; grep disk $f | wc -l; done
| awk '{t = t + $2; print $2
"\t" $1} END {print t
"\tTOTAL"}'
```

```
10 access.log
41 access.log.0
0 access.log.2010-06-03.gz
0 access.log.2010-06-04.gz
0 access.log.2010-06-05.gz
33 access.log.2010-06-06
41 access.log.2010-06-07
0 analog
0 analog_success.txt
0 error.log
0 error.log.0
0 error.log.2010-06-03.gz
0 error.log.2010-06-04.gz
0 error.log.2010-06-05.gz
0 error.log.2010-06-06
0 error.log.2010-06-07
0 hits
0 html
125 TOTAL
[perrier]$
```

Yeah that becomes a big command to remember but the idea is to make it a habit ;)

For loop here will execute the same command string in all the files and awk will do result capture and printing.



**Rohit Srivastwa**  
rohit@clubhack.com

# Prevent critical data leakage before its too late



deepranjan@chmag.in