



Email:

Petrina.Olds@team.telstra.com

Password:

\*\*\*\*\*

Sign In

Sign Up

Sign In with Telstra SSO



## Create an Account

Email:

Petrina.Olds@team.telstra.com

Password:

\*\*\*\*\*

**Create Account**

**Cancel**

[Home](#)[Upload](#)[Search](#)[Sign out](#)

# Log Normalisation Tool

[Upload Log file](#)[Search for Regex](#)[View My Contributions](#)

[Home](#)[Upload](#)[Search](#)[Sign out](#)

## My Contributions

No results found

[Home](#)[Upload](#)[Search](#)[Sign out](#)[Go back](#)

## Search Existing Regex

Search by

[Log Vendor](#)[Log Type](#)

### Results

1. Cisco Authentication Log

[View info](#)

2. Cisco Firewall Log

[View info](#)

3. Cisco System Log

[View info](#)

4. Cisco Threat Log

[View info](#)

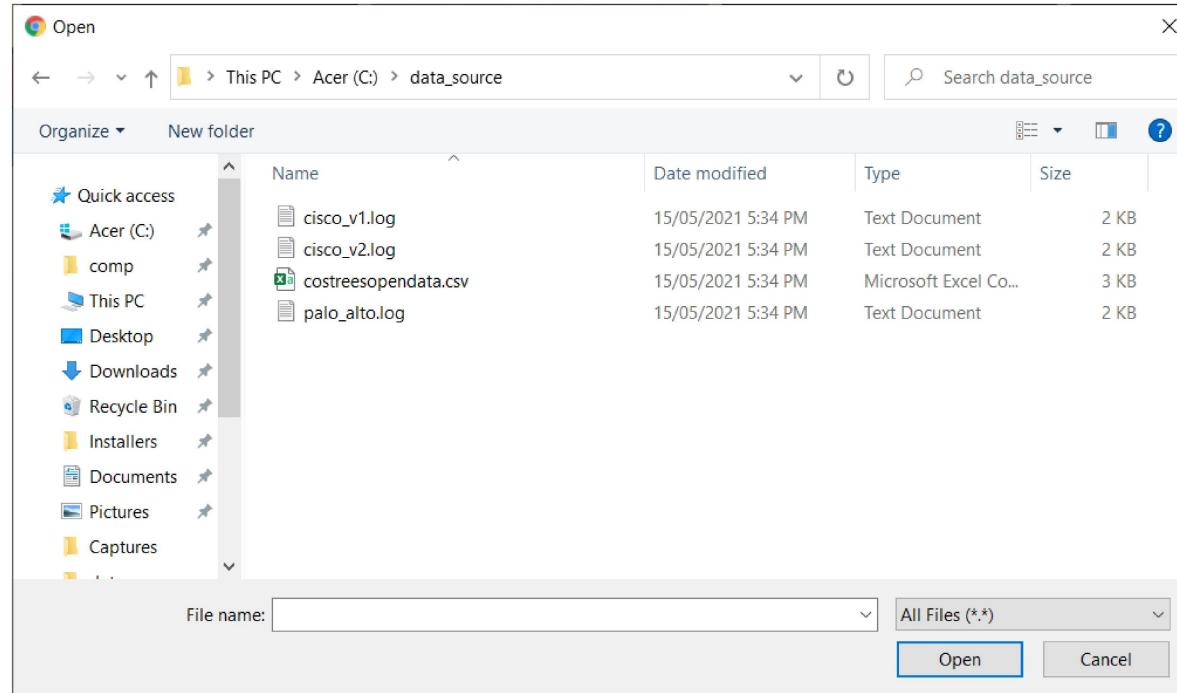
5. Cisco Traffic Log

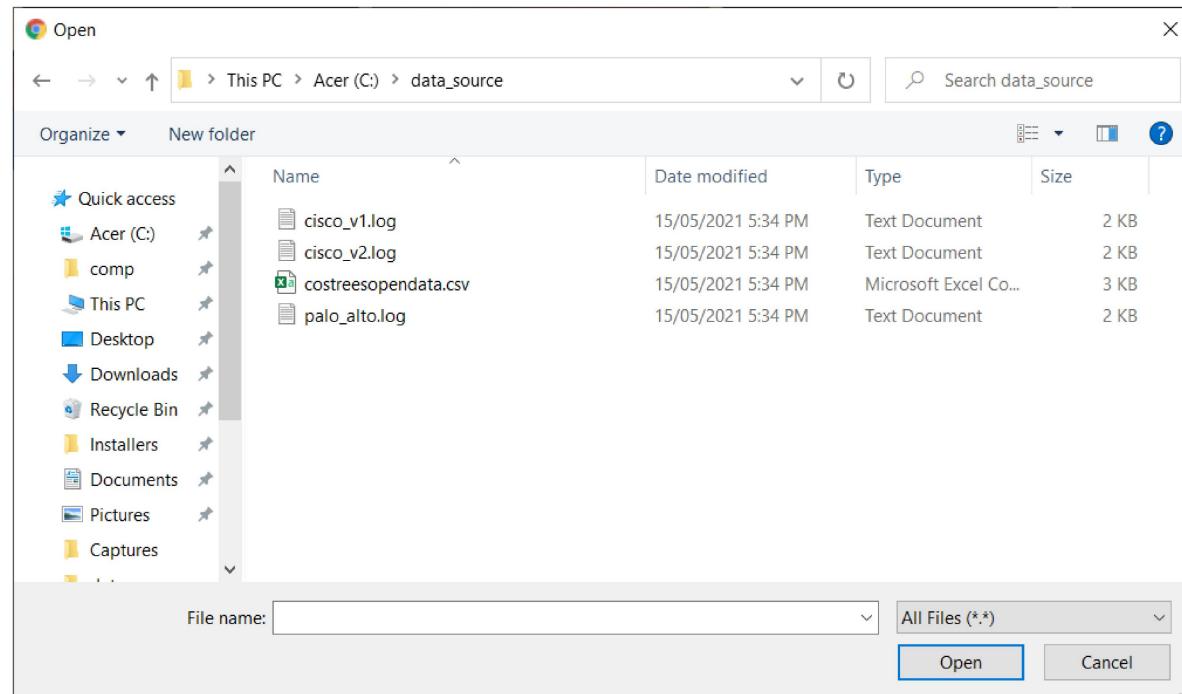
[View info](#)[Search Again](#)

[Home](#)[Upload](#)[Search](#)[Sign out](#)**Regex**

```
(?<linux_ftp_server_code>\w+\[\d{5}\]).* (?<ip_address>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})
```

[Insert](#)[Save](#)

[Home](#)[Upload](#)[Search](#)[Sign out](#)

[Home](#)[Upload](#)[Search](#)[Sign out](#)

[Home](#)[Upload](#)[Search](#)[Sign out](#)[Go back](#)

## Search Existing Regex

Cisco

Search by

[Log Vendor](#)[Log Type](#)

### Results

1. Cisco Authentication Log

[View info](#)

2. Cisco Firewall Log

[View info](#)

3. Cisco System Log

[View info](#)

4. Cisco Threat Log

[View info](#)

5. Cisco Traffic Log

[View info](#)

Search  
Again

[Home](#)[Upload](#)[Search](#)[Sign out](#)

## Cisco Traffic Log

[Log info](#)[Go back](#)

### Regular Expression

```
(?<linux_ftpd_server_date>\w+ \d{2} \d{2}:\d{2}:\d{2}) .* (?<linux_server_code>\w+\[\d{5}\]).* (?<ip_address>\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3})
```

### Sample Log Entries

```
Jun 25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
```

### Type

Traffic Log

### Vendor

Cisco

### Created By

Terence Chen

### Last Modified

28/04/2021

[Home](#)[Upload](#)[Search](#)[Sign out](#)

Regex

[Insert](#)[Save](#)

Cisco v1

[Compare another log](#)[Upload file](#)

```
06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
```

**Would you like to compare this log to a pre-existing RegEx?**

[No](#)[Yes](#)

[Home](#)[Upload](#)[Search](#)[Sign out](#)

Regex

[Insert](#)[Save](#)

Cisco v1

[Compare another log](#)[Upload file](#)

```
06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
```



[Home](#)[Upload](#)[Search](#)[Sign out](#)

Search

Filters    Log Vendor    Log Type

Recently Used

Linux FTPD Log Date

Linux FTPD Server Code

IP Address

Cancel

Search

Palo Alto

Filters

Log Vendor

Log Type

Recently Used

Linux FTPD Log Date

Linux FTPD Server Code

IP Address

Cancel



Home

# Upload

# Search

**Sign out**

# Regex

(?<linux\_ftpd\_server\_date>\w+ \d{2} \d{2}:\d{2}:\d{2}) .\* (?<linux\_ftpd\_server\_code>\w+[\d{5}\])

Insert

Save



## Regex

(?<linux\_ftpd\_log\_date>\w+ \d{2} \d{2}:\d{2}:\d{2})

Insert

Save

# Cisco v1

## Compare another log

**Upload file**

06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005

## Captured Fields

Lines: 18/18



# Regex

(?<linux\_ftpd\_server\_date>\w+ \d{2} \d{2}:\d{2}:\d{2}) .\* (?<linux\_ftpd\_server\_code>\w+\[\d{5}\])

Insert

**Save**

Cisco v1

## Compare another log

### Upload file

Lines: 18/18

06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005

# Captured Fields



# Regex

(?<linux\_ftpd\_server\_date>\w+ \d{2} \d{2}:\d{2}:\d{2}) .\* (?<linux\_ftpd\_server\_code>\w+\[\d{5}\])

Insert

Save

Cisco v1

## Compare another log

### Upload file

Lines: 18/18

06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005

# Captured Fields



# Home

## Upload

# Search

**Sign out**

# Regex

(?<linux\_ftp>\\w+\\d{2}\\d{2}:\\d{2}:\\d{2}).\*(<linux\_ftp>\\w+\\d{5}\\J).\*(?<ip\_address>\\d{1,3}.\\d{1,3}.\\d{1,3}.\\d{1,3})

Insert

Save

Cisco v1

## Compare another log

## Upload file

06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005

# Captured Fields

Lines: 18/18



# Regex

(?<linux\_ftpd\_server\_date>\w+ \d{2} \d{2}:\d{2}:\d{2}) .\* (?<linux\_ftpd\_server\_code>\w+\[\d{5}\])

Insert

Save

# Cisco v1

## Compare another log

**Upload file**

This looks like [IP Address]. Would you like to append this field to the regex?  Append field

06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005

## Captured Fields

Lines: 18/18

# Save Regex

Vendor: Cisco

Log Type: Syslog

Version: v4

Documentation: <https://cisco.com>

Save

Cancel

[Home](#)[Upload](#)[Search](#)[Sign out](#)

Regex

[Insert](#)[Save](#)

Cisco v1

[Compare another log](#)[Upload file](#)

```
06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
```



# Regex

(?<linux\_ftpdate>\w+\d{2}\d{2}\d{2}\d{2}.\*(?<linux\_ftpcode>\w+|\d{5}|).\*(<ip\_address>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})

Insert

Save

Cisco v1

## Compare another log

**Upload file**

Lines: 18/18

06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005

## Captured Fields

[Home](#)[Upload](#)[Search](#)[Sign out](#)[Regex](#)

```
(?<linux_ftpd_server_date>\w+ \d{2} \d{2}:\d{2}:\d{2}) .* (?<linux_ftpd_server_code>\w+\[\d{5}\]).* (?<ip_address>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})
```

[Insert](#)[Save](#)[Cisco v1](#)[Compare another log](#)[Upload file](#)

06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005

## Captured Fields

Lines: 1/1

linux_ftpd_log_date	linux_ftpd_server_code	ip_address
06-25 09:20:24	ftpd[31475]	210.118.170.95

[Home](#)[Upload](#)[Search](#)[Sign out](#)

Regex

```
(?<linux_ftpd_server_date>\w+ \d{2} \d{2}:\d{2}:\d{2}) .* (?<linux_server_code>\w+\[\d{5}\]).* (?<ip_address>\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3})
```

[Insert](#)[Save](#)

Cisco v1

```
06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
```

Captured Fields

Lines: 0/18

[Show sample](#)

linux_ftpd_server_date	linux_ftpd_server_code	IP Address

No Field Captured In This Format

No Field Captured In This Format

No Field Captured In This Format

[Continue to build  
Regex ->](#)

[Home](#)[Upload](#)[Search](#)[Sign out](#)**Regex**

```
(?<linux_ftpd_server_date>\w+ \d{2} \d{2}:\d{2}:\d{2}) .* (?<linux_server_code>\w+\[\d{5}\]).* (?<ip_address>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})
```

[Insert](#)[Save](#)

## Cisco v1

```
06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
```

## Sample

[Close](#)

```
Jun 25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
Jun 25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat Jun 25 09:20:24 2005
```

[Continue to build  
Regex ->](#)



# Regex

(?<linux\_ftpd\_server\_code>\w+\[\d{5}\]).\* (?<ip\_address>\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3})

Insert

Save

# Cisco v1

06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005

# Save Field

Vendor: Cisco

Log Type: Syslog

Name: IP Address

Save

Cancel

[Home](#)[Upload](#)[Search](#)[Sign out](#)

Columns

ID, , , Name, Constant, Text, Low Number, Blank, Hundreds Num, Year, One, Multiple Choice, Address, Decimal

Comma

Save

## Raw Data

```
10001,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,5,,1000,1975,1,M  
10004,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,4,,1000,1975,1,M  
10007,Fraxinus,excelsior,Golden Ash,Street Trees,12,,1200,1980,1,Mature,40 R  
10044,Malus,ioensis,Pink Crab Apple,Street Trees,3,,150,1985,1,Semi-Mature,1  
10050,Prunus,elvins,Weeping Prunus,Street Trees,5,,700,1970,1,Semi-Mature,1  
10058,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,2,,400,1970,1,Se  
10064,Melaleuca,linarifolia,Snow in Summer,Street Trees,7,,1200,1975,1,Mature  
10067,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,5,,500,1985,1,Mature  
10070,Melaleuca,linarifolia,Snow in Summer,Street Trees,5,,800,1985,1,Mature  
10090,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,5,,900,1985,1,Se  
10101,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,4,,300,1970,1,Se  
10104,Melaleuca,linarifolia,Snow in Summer,Street Trees,6,,600,1970,1,Mature  
10107,Prunus,cerasifera,Cherry Plum,Street Trees,4,,300,1970,1,Semi-Mature,1  
10110,Melaleuca,linarifolia,Snow in Summer,Street Trees,0,,0,1,Mature,33 R  
10113,Eucalyptus,viminalis,Manna Gum,Street Trees,5,,300,1970,1,Semi-Mature  
10121,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,4,,300,1970,1,Se  
10127,Lophostemon,confertus,Queensland Box Brush,Street Trees,4,,300,199  
10130,Lophostemon,confertus,Queensland Box Brush,Street Trees,2,,100,199  
Tree_ID,Genus_Desc,Spec_Desc,Common_Name,Location_Type,Height_m,Car
```

## Field Suggestions

ID	Text	Text	Name
10001	Melaleuca	stypheliodes	Prickly Paperback
10004	Melaleuca	stypheliodes	Prickly Paperback
10007	Fraxinus	excelsior	Golden Ash
10044	Malus	ioensis	Pink Crab Apple
10050	Prunus	elvins	Weeping Prunus
10058	Melaleuca	stypheliodes	Prickly Paperback
10064	Melaleuca	linarifolia	Snow in Summer
10067	Melaleuca	stypheliodes	Prickly Paperback
10070	Melaleuca	linarifolia	Snow in Summer
10090	Melaleuca	stypheliodes	Prickly Paperback
10101	Melaleuca	stypheliodes	Prickly Paperback
10104	Melaleuca	linarifolia	Snow in Summer
10107	Prunus	cerasifera	Cherry Plum
10110	Melaleuca	linarifolia	Snow in Summer
10113	Eucalyptus	viminalis	Manna Gum
10121	Melaleuca	stypheliodes	Prickly Paperback
10127	Lophostemon	confertus	Queensland Box Brush
10130	Lophostemon	confertus	Queensland Box Brush
Tree_ID	Genus_Desc	Spec_Desc	Common_Name

[Home](#)[Upload](#)[Search](#)[Sign out](#)

Columns

Tab

[Save](#)

## Raw Data

10001,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,5,,1000,1975,1,M  
10004,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,4,,1000,1975,1,M  
10007,Fraxinus,excelsior,Golden Ash,Street Trees,12,,1200,1980,1,Mature,40 R  
10044,Malus,ioensis,Pink Crab Apple,Street Trees,3,,150,1985,1,Semi-Mature,1  
10050,Prunus,elvins,Weeping Prunus,Street Trees,5,,700,1970,1,Semi-Mature,1  
10058,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,2,,400,1970,1,Se  
10064,Melaleuca,linarifolia,Snow in Summer,Street Trees,7,,1200,1975,1,Mature  
10067,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,5,,500,1985,1,Mature  
10070,Melaleuca,linarifolia,Snow in Summer,Street Trees,5,,800,1985,1,Mature  
10090,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,5,,900,1985,1,Se  
10101,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,4,,300,1970,1,Se  
10104,Melaleuca,linarifolia,Snow in Summer,Street Trees,6,,600,1970,1,Mature  
10107,Prunus,cerasifera,Cherry Plum,Street Trees,4,,300,1970,1,Semi-Mature,1  
10110,Melaleuca,linarifolia,Snow in Summer,Street Trees,0,,0,0,1,Mature,33 Ro  
10113,Eucalyptus,viminalis,Manna Gum,Street Trees,5,,300,1970,1,Semi-Mature  
10121,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,4,,300,1970,1,Se  
10127,Lophostemon,confertus,Queensland Box Brush,Street Trees,4,,300,199  
10130,Lophostemon,confertus,Queensland Box Brush,Street Trees,2,,100,199  
Tree\_ID,Genus\_Desc,Spec\_Desc,Common\_Name,Location\_Type,Height\_m,Car

## Field Suggestions

Text

10001 , Melaleuca , stypheliodes , Prickly Paperback , Street Trees  
10004 , Melaleuca , stypheliodes , Prickly Paperback , Street Trees  
10007 , Fraxinus , excelsior , Golden Ash , Street Trees , 12 , , 1200  
10044 , Malus , ioensis , Pink Crab Apple , Street Trees , 3 , , 150 , 1985  
10050 , Prunus , elvins , Weeping Prunus , Street Trees , 5 , , 700 , 1970  
10058 , Melaleuca , stypheliodes , Prickly Paperback , Street Trees  
10064 , Melaleuca , linarifolia , Snow in Summer , Street Trees , 7  
10067 , Melaleuca , stypheliodes , Prickly Paperback , Street Trees  
10070 , Melaleuca , linarifolia , Snow in Summer , Street Trees , 5  
10090 , Melaleuca , stypheliodes , Prickly Paperback , Street Trees  
10101 , Melaleuca , stypheliodes , Prickly Paperback , Street Trees  
10104 , Melaleuca , linarifolia , Snow in Summer , Street Trees , 6  
10107 , Prunus , cerasifera , Cherry Plum , Street Trees , 4 , , 300 , 1970  
10110 , Melaleuca , linarifolia , Snow in Summer , Street Trees , 0  
10113 , Eucalyptus , viminalis , Manna Gum , Street Trees , 5 , , 300  
10121 , Melaleuca , stypheliodes , Prickly Paperback , Street Trees  
10127 , Lophostemon , confertus , Queensland Box Brush , Street Trees  
10130 , Lophostemon , confertus , Queensland Box Brush , Street Trees  
Tree\_ID,Genus\_Desc,Spec\_Desc,Common\_Name,Location\_Type,He

[Home](#)[Upload](#)[Search](#)[Sign out](#)Columns .....  
Space   

## Raw Data

10001,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,5,,1000,1975,1,M  
10004,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,4,,1000,1975,1,M  
10007,Fraxinus,excelsior,Golden Ash,Street Trees,12,,1200,1980,1,Mature,40 R  
10044,Malus,ioensis,Pink Crab Apple,Street Trees,3,,150,1985,1,Semi-Mature,1  
10050,Prunus,elvins,Weeping Prunus,Street Trees,5,,700,1970,1,Semi-Mature,1  
10058,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,2,,400,1970,1,Se  
10064,Melaleuca,linarifolia,Snow in Summer,Street Trees,7,,1200,1975,1,Mature  
10067,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,5,,500,1985,1,Mature  
10070,Melaleuca,linarifolia,Snow in Summer,Street Trees,5,,800,1985,1,Mature  
10090,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,5,,900,1985,1,Se  
10101,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,4,,300,1970,1,Se  
10104,Melaleuca,linarifolia,Snow in Summer,Street Trees,6,,600,1970,1,Mature  
10107,Prunus,cerasifera,Cherry Plum,Street Trees,4,,300,1970,1,Semi-Mature,1  
10110,Melaleuca,linarifolia,Snow in Summer,Street Trees,0,,0,0,1,Mature,33 Ro  
10113,Eucalyptus,viminalis,Manna Gum,Street Trees,5,,300,1970,1,Semi-Mature  
10121,Melaleuca,stypheliodes,Prickly Paperback,Street Trees,4,,300,1970,1,Se  
10127,Lophostemon,confertus,Queensland Box Brush,Street Trees,4,,300,199  
10130,Lophostemon,confertus,Queensland Box Brush,Street Trees,2,,100,199  
Tree\_ID,Genus\_Desc,Spec\_Desc,Common\_Name,Location\_Type,Height\_m,Car

## Field Suggestions

Text

10001 , Melaleuca , stypheliodes , Prickly  
10004 , Melaleuca , stypheliodes , Prickly  
10007 , Fraxinus , excelsior , Golden  
10044 , Malus , ioensis , Pink  
10050 , Prunus , elvins , Weeping  
10058 , Melaleuca , stypheliodes , Prickly  
10064 , Melaleuca , linarifolia , Snow  
10067 , Melaleuca , stypheliodes , Prickly  
10070 , Melaleuca , linarifolia , Snow  
10090 , Melaleuca , stypheliodes , Prickly  
10101 , Melaleuca , stypheliodes , Prickly  
10104 , Melaleuca , linarifolia , Snow  
10107 , Prunus , cerasifera , Cherry  
10110 , Melaleuca , linarifolia , Snow  
10113 , Eucalyptus , viminalis , Manna  
10121 , Melaleuca , stypheliodes , Prickly  
10127 , Lophostemon , confertus , Queensland  
10130 , Lophostemon , confertus , Queensland  
Tree\_ID,Genus\_Desc,Spec\_Desc,Common\_Name,Location\_Type,He:

[Home](#)[Upload](#)[Search](#)[Sign out](#)[Regex](#)

(?&lt;linux\_ftpd\_server\_date&gt;\w+ \d{2} \d{2}:\d{2}:\d{2}) .\* (?&lt;linux\_ftpd\_server\_code&gt;\w+[\d{5}\]) .\* (?&lt;ip\_address&gt;\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})

[Insert](#)[Save](#)[Cisco v1](#)[Compare another log](#)[Upload file](#)

```
06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
```

## Captured Fields

Lines: 18/18

linux_ftpd_log_date	linux_ftpd_server_code	*ip_address
06-25 09:20:24	ftpd[31475]	210.118.170.95

\*The field is unsaved ...

[Home](#)[Upload](#)[Search](#)[Sign out](#)

Regex

`(?<linux_ftpd_server_date>\w+ \d{2} \d{2}:\d{2}) .* (?<linux_ftpd_server_code>\w+\[\d{5}\]).* (?<ip_address>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})`[Insert](#)[Save](#)

Cisco v1

[Compare another log](#)[Upload file](#)

```
06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005
```

## Captured Fields

Lines: 18/18

linux_ftpd_log_date	linux_ftpd_server_code	*ip_address
06-25 09:20:24	ftpd[31475]	210.118.170.95

\*The field is unsaved ...

Save the captured group for this field?

[Yes](#)[No](#)



# Regex

(?<linux\_ftp\_server\_date>\w+\.\d{2}\.\d{2}:\d{2}:\d{2}).\*(?<linux\_ftp\_server\_code>\w+|\{\d{5}\}).\*(?<ip\_address>\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3})

## Insert

**Save**

# Cisco v1

## Compare another log

**Upload file**

06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005

## Captured Fields

Lines: 18/18



Home

## Upload

## Search

**Sign out**

# Regex

## Insert

**Save**

06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005

## Complete Comparison



Home

## Upload

# Search

**Sign out**

# Regex

## Insert

Save

06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005

## Complete Comparison



# Regex

(?<linux\_ftpd\_server\_date>\w+ \d{2} \d{2}:\d{2}:\d{2})

Insert

Save

06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005



## Complete Comparison



# Regex

(?<linux\_ftpd\_server\_date>\w+ \d{2} \d{2}:\d{2}:\d{2}) .\* (?<linux\_ftpd\_server\_code>\w+[\d{5}\])

Insert

Save

06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005

 format changed in this field

## Complete Comparison



# Regex

(?<palo\_alto\_ftpd\_server\_date>\w+ \d{2}\.\d{2}\.\d{2} \d{2}.\* (?<palo\_alto\_ftpd\_server\_code>\w+\[(\d{5})\]).\* (?<ip\_address>\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3})

Insert

Save

06-25 09:20:24 combo ftpd[31475]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31477]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31474]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31476]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31473]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31467]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31470]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31465]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31472]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31468]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31463]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31471]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31469]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31462]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31464]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31466]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31461]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005  
06-25 09:20:24 combo ftpd[31460]: connection from 210.118.170.95 () at Sat 06-25 09:20:24 2005

 format changed in this field

## Complete Comparison