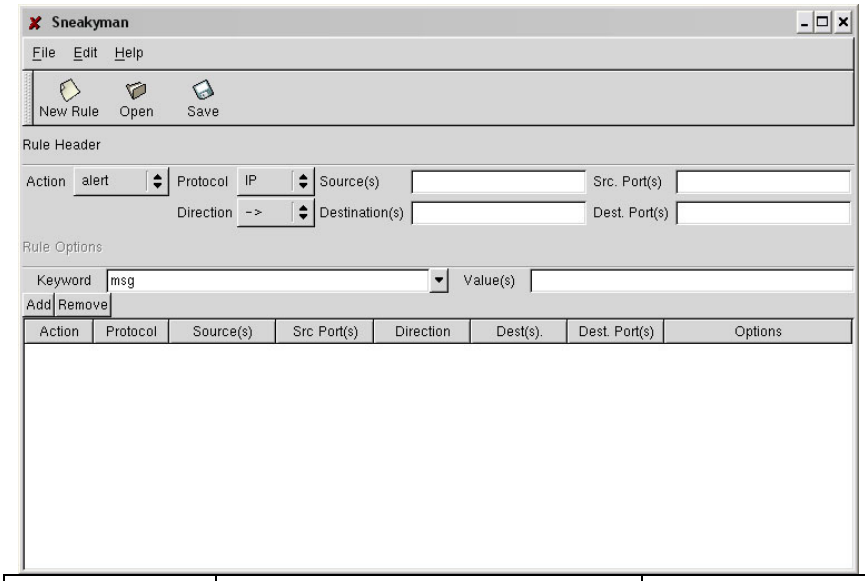
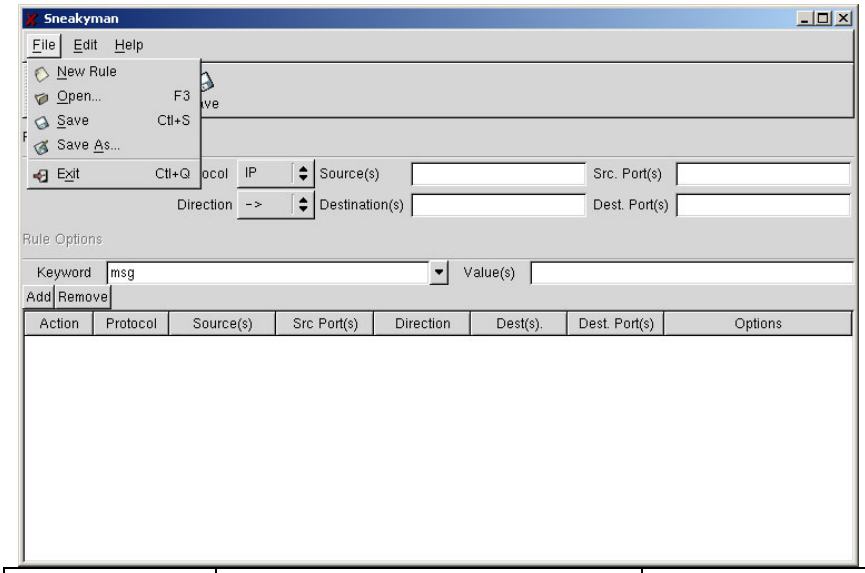
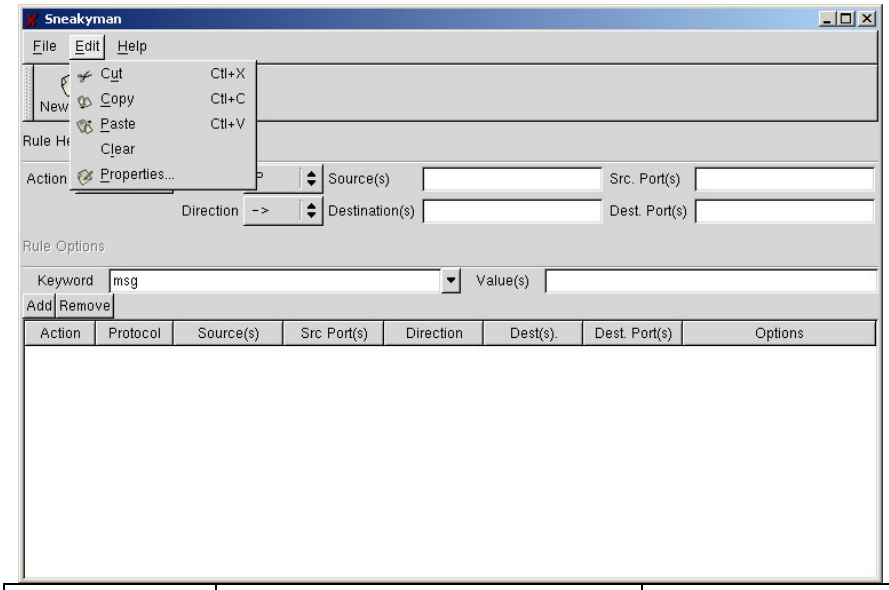
**Sneakyman Functional Specs v.01**



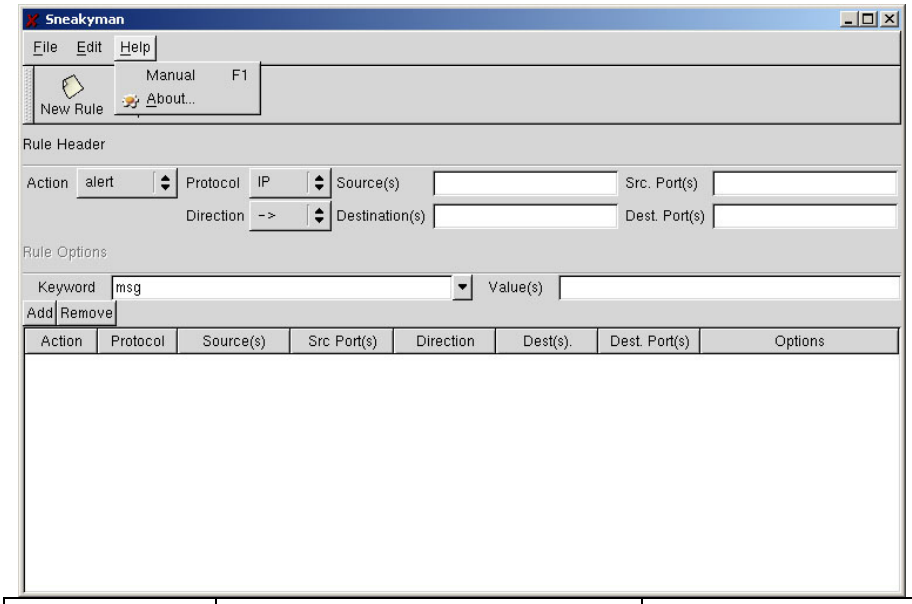

| Button | Function | Action |
|---|---|---|
| New Rule | Creates New Rule | |
| Open | Opens Different Ruleset File | Spawns File Selection dialog |
| Save | Save current Ruleset files | Spawns Save dialog if file name unknown |



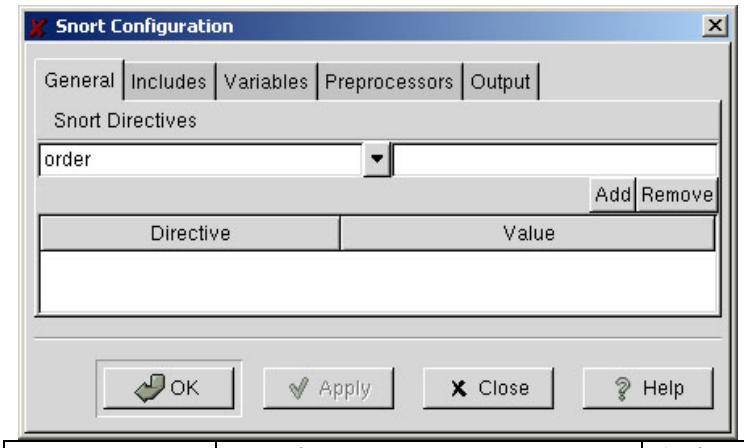

| Button | Function | Action |
|---|---|---|
| New Rule | Creates New Rule | |
| Open… | Opens Different Ruleset File | Spawns File Selection dialog |
| Save | Save current Ruleset files | Spawns Save dialog if file name unknown |
| Save As… | Save Ruleset to a different file | Spawns Save As… dialog |
| Exit | Exits application | Closes program – check unsaved changes. |



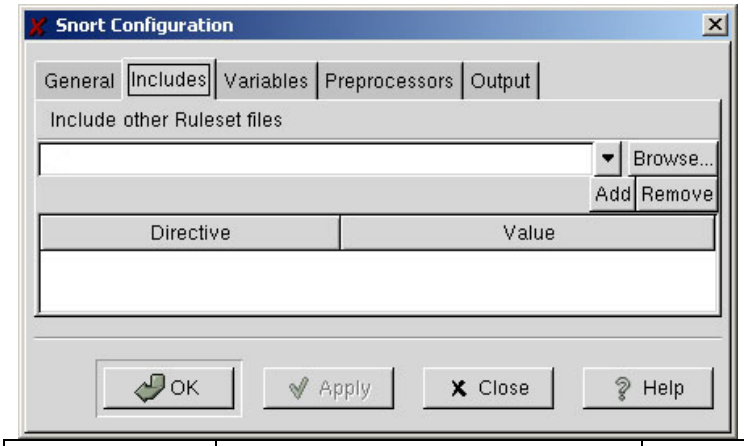

| Button | Function | Action |
|---|---|---|
| Cut | Cuts selected text | Move to clipboard |
| Copy | Copy selected text | Copy to clipboard |
| Paste | Pastes selected text | Paste from clipboard |
| Clear | Clear text | Removes text/settings from all items |
| Properties | General Snort Configuration | Open Snort Options modal dialog |




| Button | Function | Action |
|---|---|---|
| Manual | Help system for application | Open gnome help browser for Sneakyman |
| About | Program Information | Display About window. |

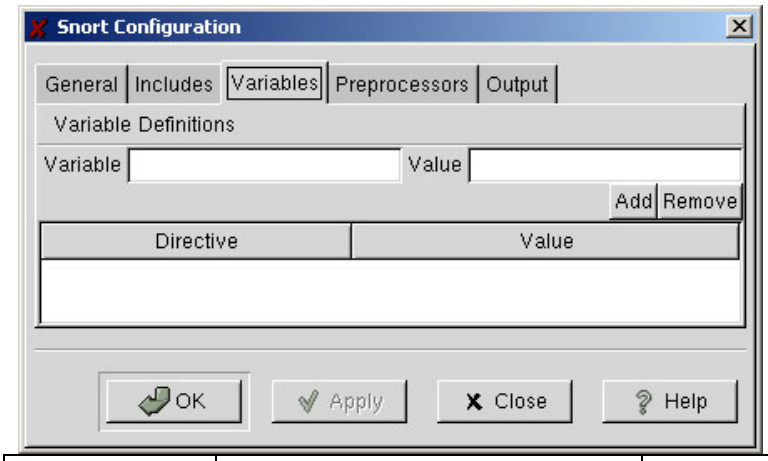



| Button | Function | Action |
|---|---|---|
| Directive field | Contains selectable list of snort directives. | Click dropdown and select directive, or type custom one in. |
| Value field | Values for selected directive | Generic text entry |
| Add | Add directive/value pair to list | Click and directive/value pair is added to columned list below |
| Remove | Remove selected pair from list | Click pair in columned list and click to remove |
| Columned list | Display directive/value pairs | Singly-selectable list of directive/value pairs |
| OK | Commit changes and close window | Save changes for later writing and close window |
| Apply | Commit changes | Save changes for later writing |
| Close | Close window – discard changes | Discard all changes made, destroy window. |
| Help | Provide Context-sensitive help | Display help window for current configuration item. |

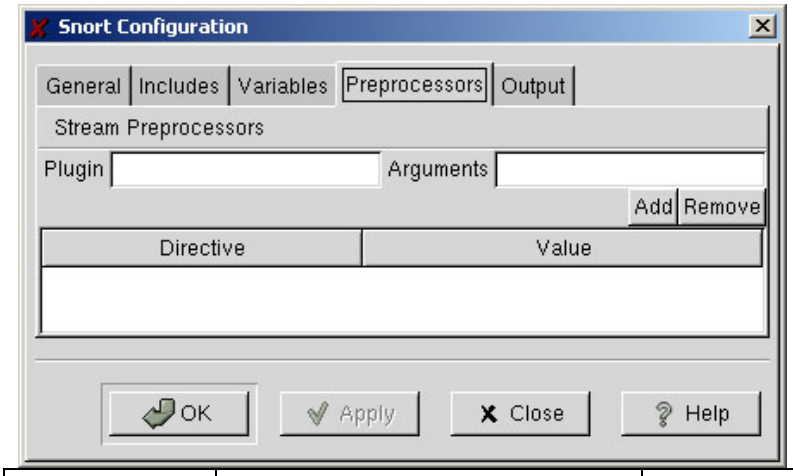



| Button | Function | Action |
|---|---|---|
| Entry line | Contains selectable list of snort directives. | Click dropdown and select directive, or type custom one in. |
| Browse | Allows user to select ruleset file | Opens generic file selection dialog |
| Add | Add ruleset file to list | Click and directive/value pair is added to columned list below |
| Remove | Remove selected pair from list | Click pair in columned list and click to remove |
| Columned list | Display directive/value pairs | Singly-selectable list of directive/value pairs |

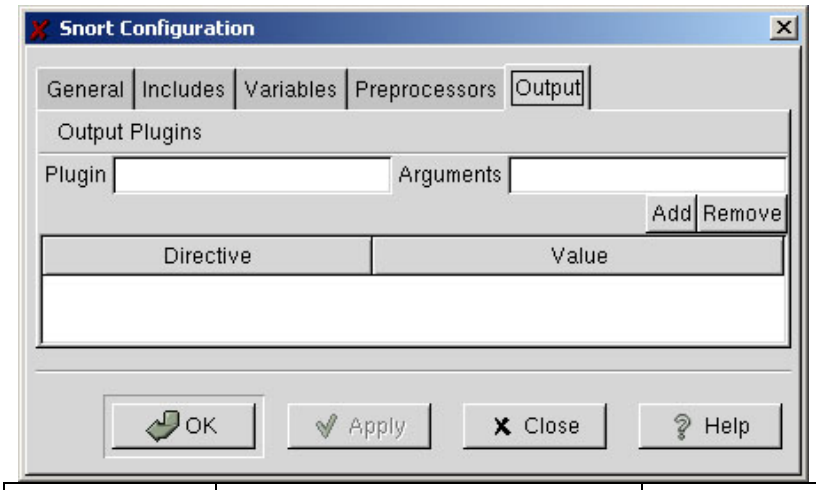
| | | |
|---|---|---|
| OK | Commit changes and close window | Save changes for later writing and close window |
| Apply | Commit changes | Save changes for later writing |
| Close | Close window – discard changes | Discard all changes made, destroy window. |
| Help | Provide Context-sensitive help | Display help window for current configuration item. |




| **Button** | **Function** | **Action** |
|---|---|---|
| Variable field | Text field for generic variable definitions. | Click dropdown and select variable, or type custom one in. |
| Value field | Values for selected variable | Generic text entry |
| Add | Add variable/value pair to list | Click and variable/value pair is added to columned list below |
| Remove | Remove selected pair from list | Click pair in columned list and click to remove |
| Columned list | Display variable/value pairs | Singly-selectable list of variable/value pairs |
| OK | Commit changes and close window | Save changes for later writing and close window |
| Apply | Commit changes | Save changes for later writing |
| Close | Close window – discard changes | Discard all changes made, destroy window. |
| Help | Provide Context-sensitive help | Display help window for current configuration item. |

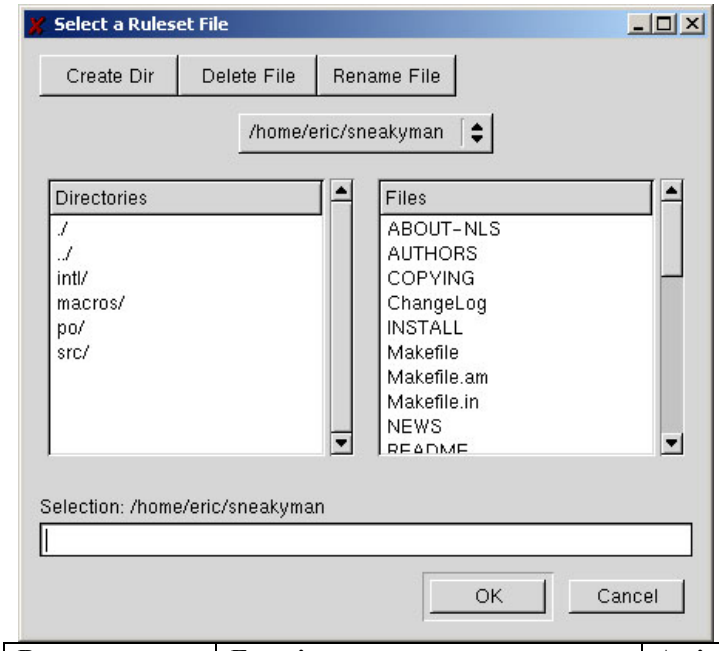



| Button | Function | Action |
|---|---|---|
| Preprocessor field | Text field to enter stream Preprocessors. | Click dropdown and select Preprocessor, or type custom one in. |
| Value field | Values for selected Preprocessor | Generic text entry |
| Add | Add Preprocessor/value pair to list | Click and Preprocessor/value pair is added to columned list below |
| Remove | Remove selected pair from list | Click pair in columned list and click to remove |
| Columned list | Display Preprocessor/value pairs | Singly-selectable list of Preprocessor/value pairs |
| OK | Commit changes and close window | Save changes for later writing and close window |
| Apply | Commit changes | Save changes for later writing |
| Close | Close window – discard changes | Discard all changes made, destroy window. |
| Help | Provide Context-sensitive help | Display help window for current configuration item. |




| Button | Function | Action |
|---|---|---|
| Output field | Text field to enter stream Outputs. | Click dropdown and select Preprocessor, or type custom one in. |
| Value field | Values for selected Output | Generic text entry |
| Add | Add Preprocessor/value pair to list | Click and Preprocessor/value pair is added to columned list below |
| Remove | Remove selected pair from list | Click pair in columned list and click to remove |

| | | |
|---|---|---|
| Columned list | Display Output/value pairs | Singly-selectable list of Output/value pairs |
| OK | Commit changes and close window | Save changes for later writing and close window |
| Apply | Commit changes | Save changes for later writing |
| Close | Close window – discard changes | Discard all changes made, destroy window. |
| Help | Provide Context-sensitive help | Display help window for current configuration item. |




| **Button** | **Function** | **Action** |
|---|---|---|
| OK | OK File Selection | Return selected file to calling application segment |
| Cancel | Cancel File Selection | Remove window with no selection |


| **Button** | **Function** | **Action** |
|---|---|---|
| OK | Exits About dialog | Closes Window |

**Initial Data Management**

**Rulesets:**

```
typedef struct completeRule {
        gchar *action;
        gchar *src_ip;                  /* all IP and port information can be
        gchar *src_port;                    comma-delimited and ranged with -
        gchar *dest_ip;
        gchar *dest_port;
        gchar *protocol;
        gchar  direction[3];
        GHashTable *rule_options;       // keyword strings for retrieval keys.
};
```

**Options:**

```
typedef struct  optionType {
        gchar *keyword;
        gchar *arguments;
};
```

**Functionality**

**Initial Release**

- Creation of complex rulesets using pre-defined ruletypes.
- Pre-defined protocols
- Basic rule-unrelated configuration of Snort.
- Help System
- Distribution through tar/gzip'ed source tree.

**Future Release(s)**

- Non-NIDS configuration options.
- User-definable ruletypes and protocols.
- Keyword-specific tooltips.
- Additional changes related to any new snort releases.
- Saved configuration options (default rules directory, full GNOME installation into menu, icon design, etc.).
- Improve error-checking and possible application speed-ups.
- Added distribution of an RPM (source and binary).

**Projected Timelines**

- Initial UI and Design Specifications: February 11th, 2002
- Alpha Release 0.98 (initial testing stage): February 31st, 2002
- Beta Release 0.99 (mostly bug fixes, last chance for major UI changes): March 14th, 2002.
- Version 1.0: March 21st, 2002.
- New alpha 1.08 (new functionality introduced): April 4th, 2002.
- Beta Release 1.09 (feature freeze, bug fixes): April 11th, 2002.
- Final project version 1.1: April 18th, 2002
- Program upkeep, new unplanned functionality, user management (bug tracking, mailing lists, etc), documentation, final paper: April 19th – May 10th.