BRO AND BRO-IDS

File Extraction

HTTP, FTP, SMTP, IRC

Presented by
Liam Randall
2013-2-25

ABOUT ME

History

- 17 Years Consulting (1995)
- BS in CS from XU
- Dozens of Vender Certs
- Speak/Train- Shmoocon, Skydogcon
- “Applied NSM” Summer of 2013

- Bro-IDS
- SecurityOnion

- Liam.Randall@gmail.com
- @Hectaman Twitter/IRC

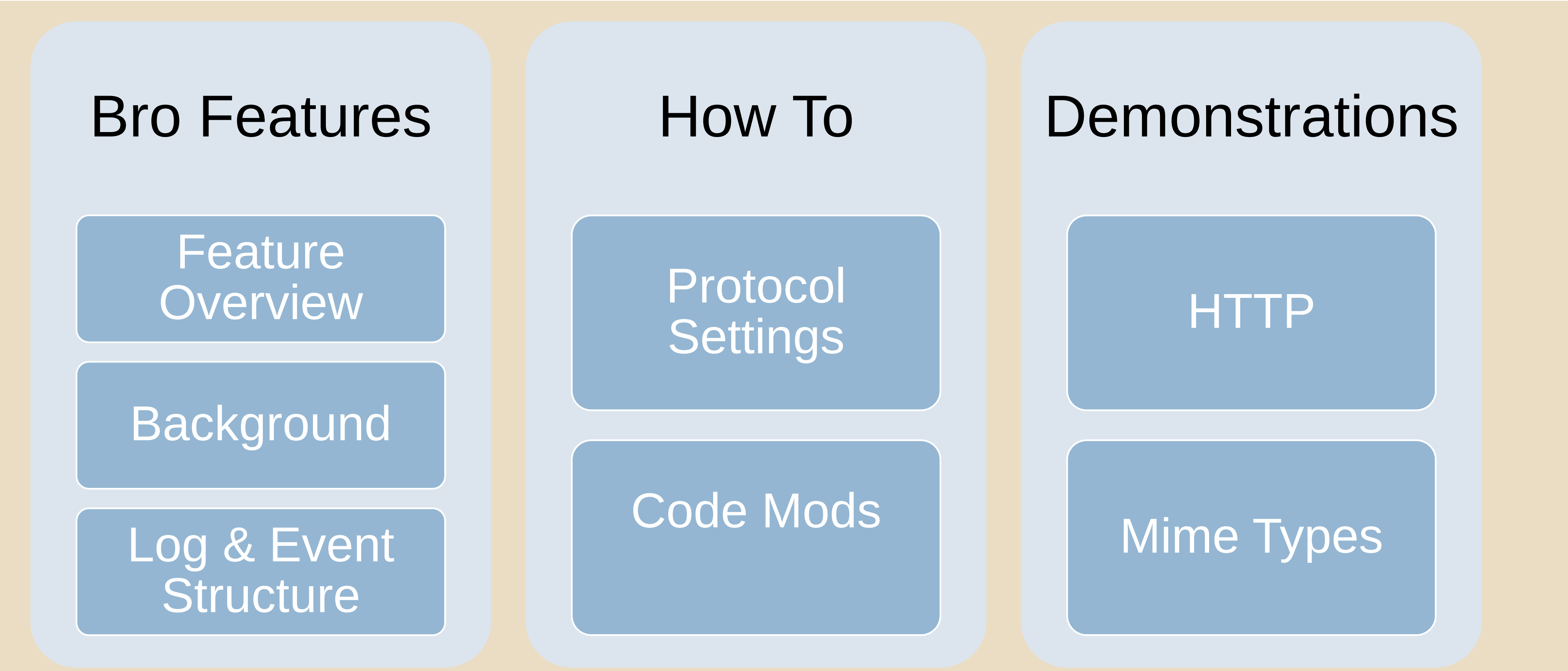
LINKS

Github
github/liamrandall

#Bro_IDS
@Hectaman
@Bro_IDS

http://bro-ids.org

PRESENTATION OVERVIEW



Bro Features

- Feature Overview
- Background
- Log & Event Structure

How To

- Protocol Settings
- Code Mods

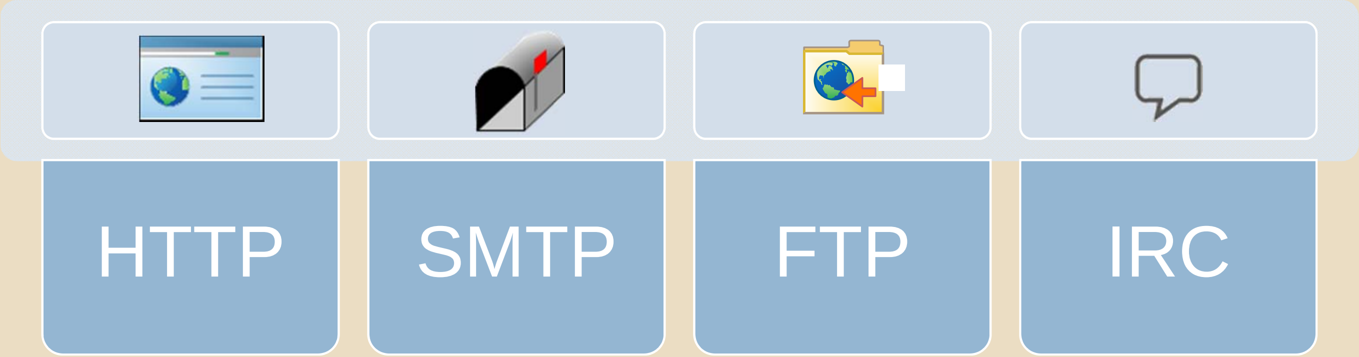
Demonstrations

- HTTP
- Mime Types

PROTOCOLS

Why File Extraction

+ Archive by type
+ Further Analysis
+ ??? Detection

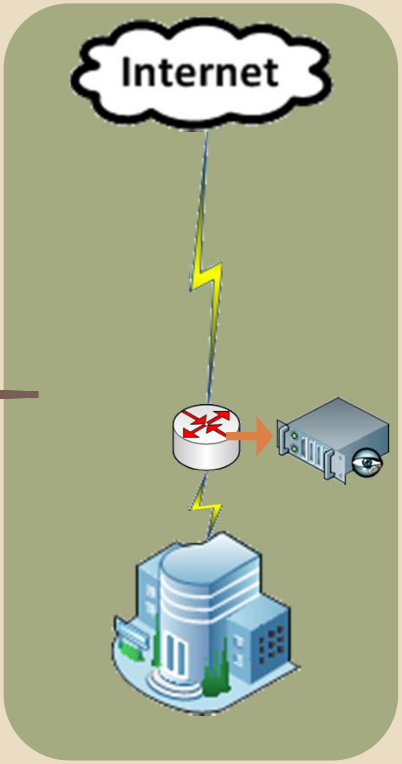


HTTP

SMTP

FTP

IRC

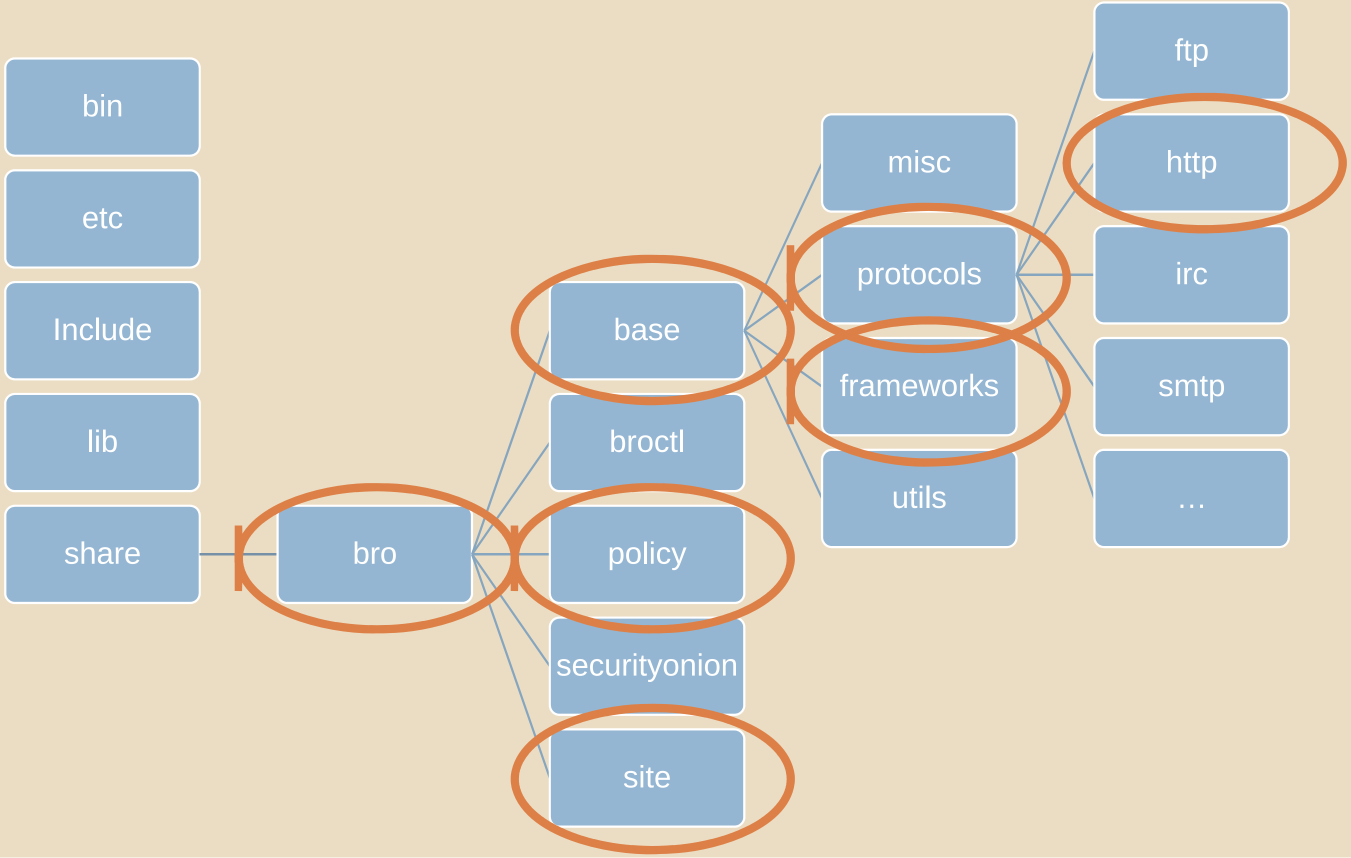


FOLLOW ALONG

Documentation

http://www.bro-ids.org/documentation/quickstart.html

DIRECTORY STRUCTURE



bin

etc

Include

lib

share

bro

base

broctl

policy

securityonion

site

misc

protocols

frameworks

utils

ftp

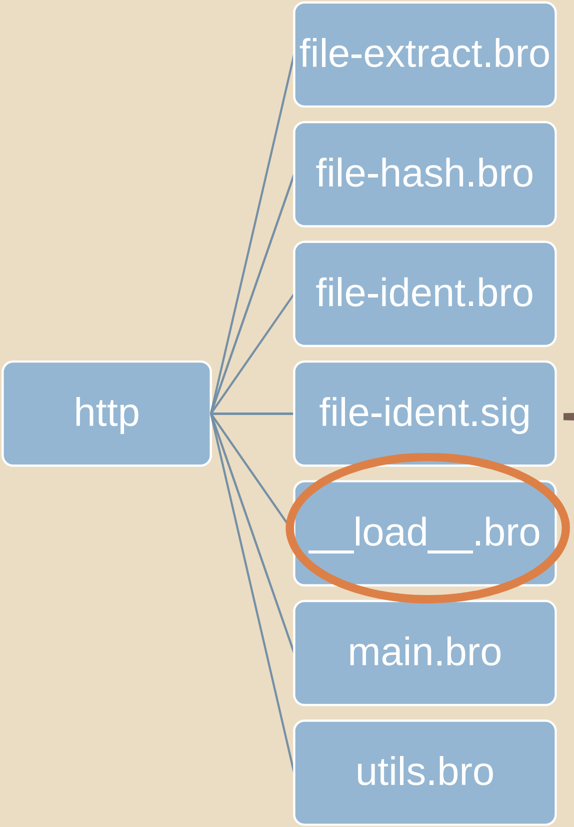
http

irc

smtp

…

BASE/PROTOCOLS/HTTP



http

file-extract.bro

file-hash.bro

file-ident.bro

file-ident.sig

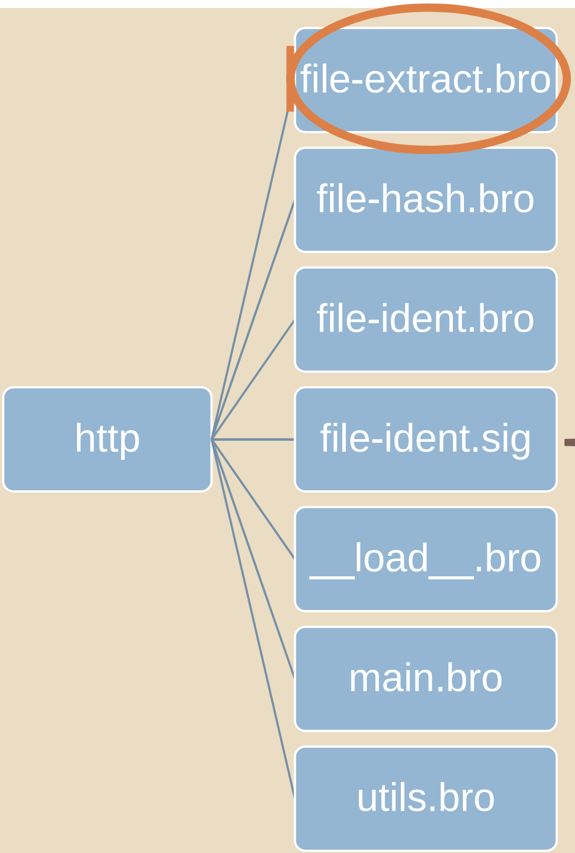
__load__.bro

main.bro

utils.bro

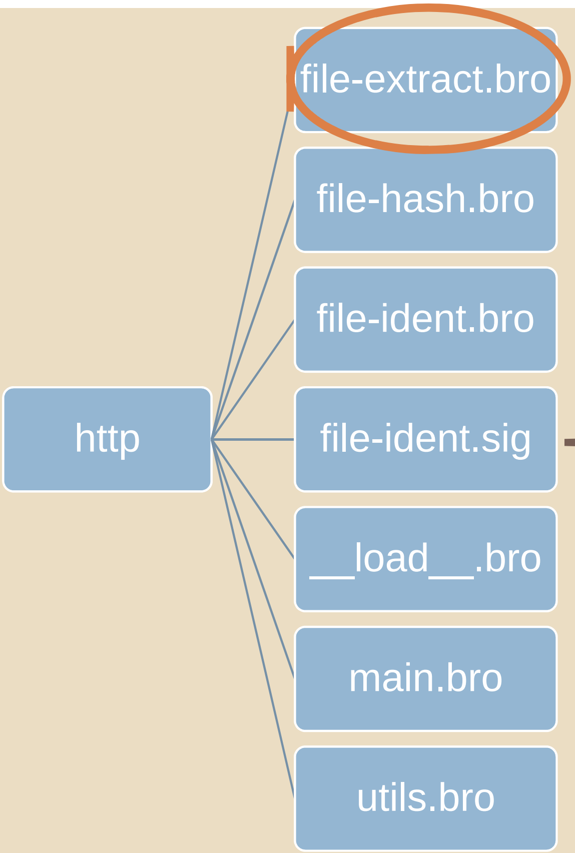
```
@load ./main
@load ./utils
@load ./file-ident
@load ./file-hash
@load ./file-extract
```

FILE EXTRACTION



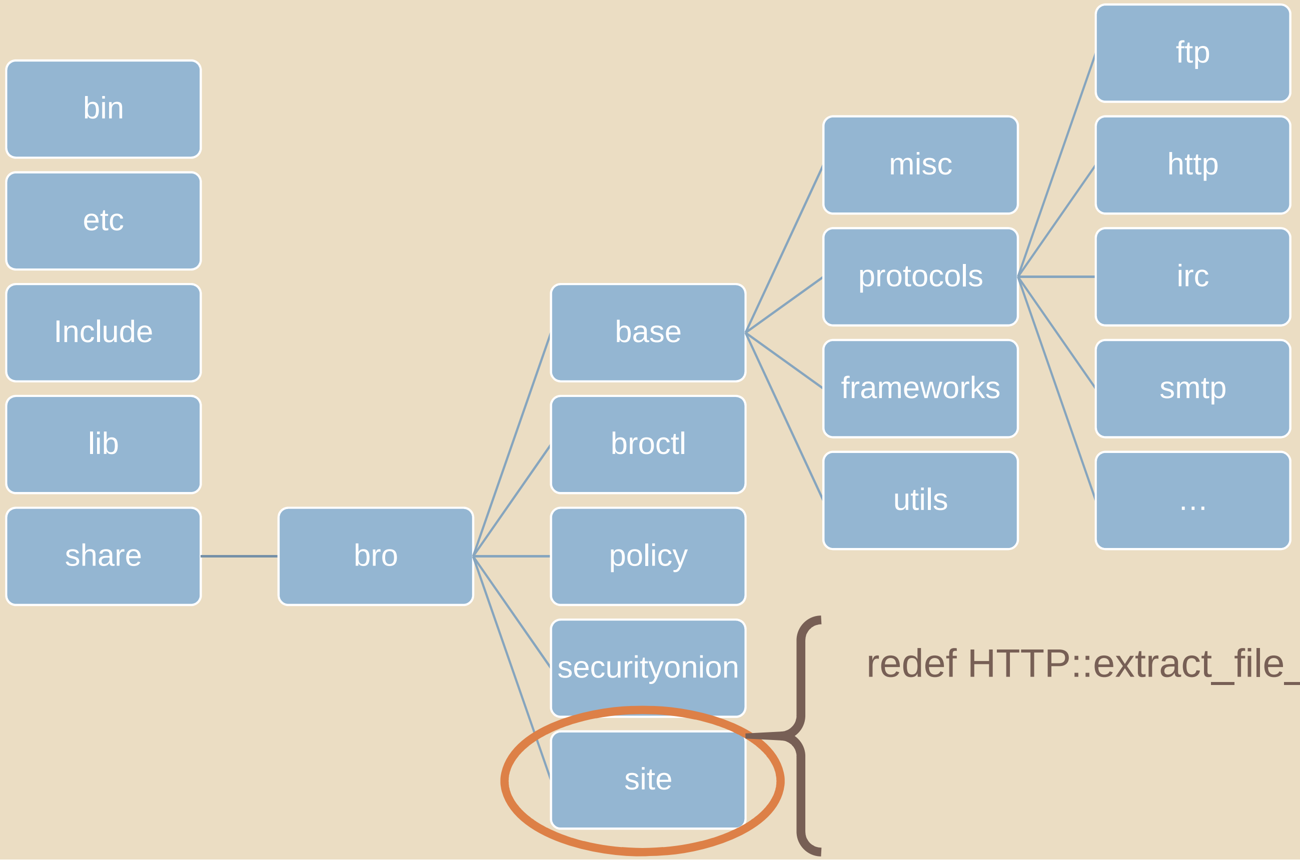
```
..
export {
    ## Pattern of file mime types to extract
    const extract_file_types = /NO_DEFAULT/ &redef;

    ## on-disk prefix for files to be extracted from HTTP
    const extraction_prefix = "http-item" &redef;

    redef record Info += {
      ## On-disk file where the response body was extracted to.
      extraction_file:  file &log &optional;

      ## Indicates if the response body extracted or not
      extract_file:     bool &default=F;
    };
}
..
```

CONST &REDEF



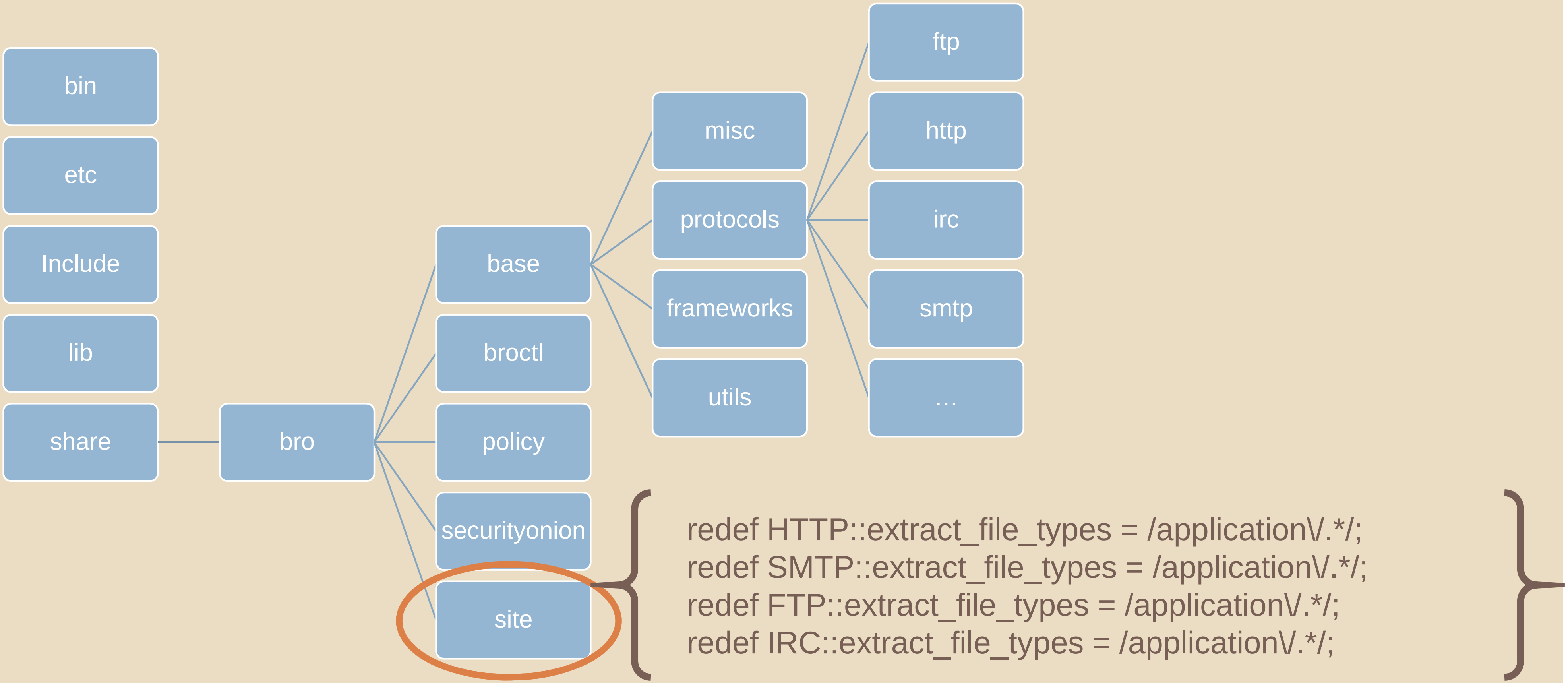
```
..
export {
    ## Pattern of file mime types to extract
    const extract_file_types = /NO_DEFAULT/ &redef;

    ## on-disk prefix for files to be extracted from HTTP
    const extraction_prefix = "http-item" &redef;

    redef record Info += {
      ## On-disk file where the response body was extracted to.
      extraction_file:  file &log &optional;

      ## Indicates if the response body extracted or not
      extract_file:     bool &default=F;
    };
}
..
```

HTTP MIME TYPES


bin
etc
Include
lib
share
bro
base
broctl
policy
securityonion
site
misc
protocols
frameworks
utils
ftp
http
irc
smtp
…

```
redef HTTP::extract_file_types = /application\/.*/;
```

OTHER MIME TYPES



```
redef HTTP::extract_file_types = /application\/.*/;
redef SMTP::extract_file_types = /application\/.*/;
redef FTP::extract_file_types = /application\/.*/;
redef IRC::extract_file_types = /application\/.*/;
```

TO DO

http://www.freeformatter.com/mime-types-list.html

- Pro’s & Con’s to various Mime Type Extractions
- What other types of things can be redefined?