

Zulu: A Command Line Wireless Frame Injector

Damon McCoy, Anmol Sheth

Contact: Damon.McCoy@Colorado.edu

Department of Computer Science
University of Colorado at Boulder



What is Zulu good for?

- Injecting custom frames
 - Probe a wireless network for security holes
 - Debugging a wireless Network
 - Launching De-authentication and De-association attacks
 - Testing wireless device drivers



What is Zulu?

- A command line tool to inject wireless frames
- Allows the user to set and unset most fields in a wireless frame
- Supports 20 command line options
- Works with Madwifi-ng drivers
- Includes code from lorcon to allow the channel and essid to be set

The word "ZULU" is written in a stylized, blue, serif font with a slight shadow effect. The letters are bold and have a classic, slightly ornate appearance.

What is the goal of Zulu?

- The vision behind Zulu
 - Easy to use
 - Command line wireless frame injection tool
 - An hping tool for the wireless world
 - Minimal required options good default values
 - Plenty of options to customize frames
 - Requires no programming knowledge
 - Works with unmodified drivers



Command Line Options

Usage: zulu -t <type of frame> -i <interface> [options]

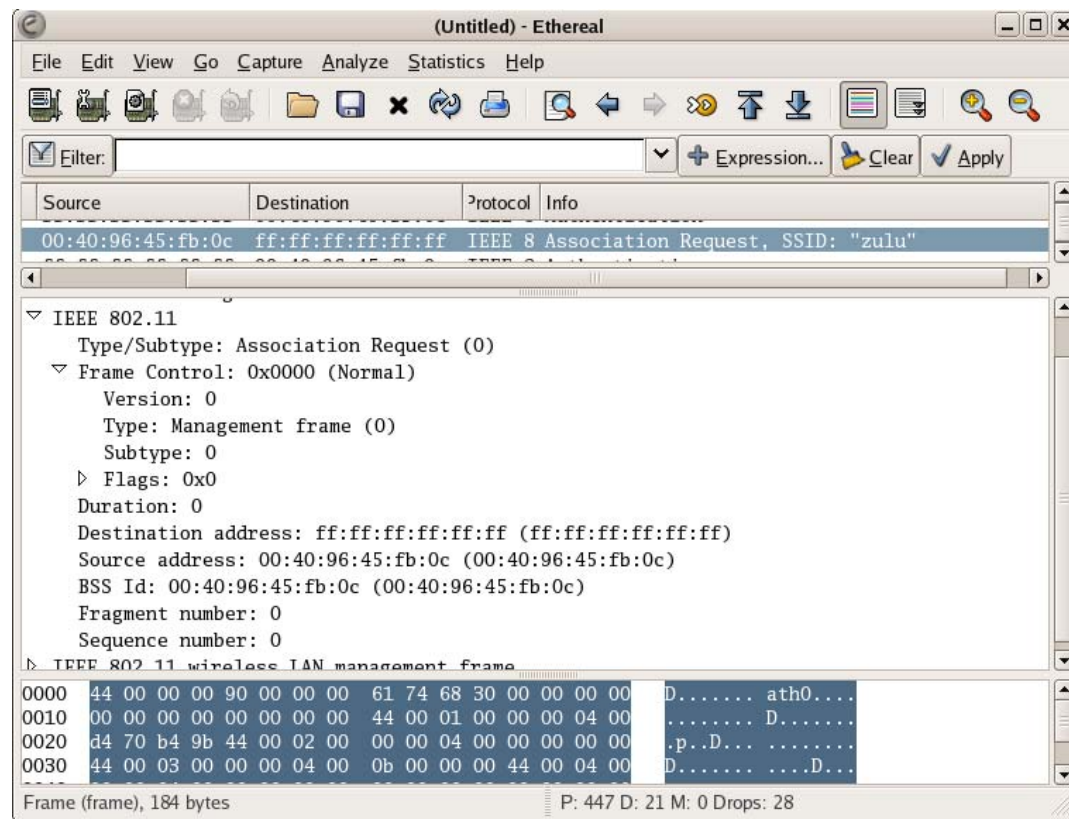
Optional Arguments

-s <src mac>	--duration <duration>
-d <dest mac>	--to_ap
-n <# of frames to send>	--from_ap
--delay <n>	--adhoc
-w -r -p -m -o	--bridge
-f <fragement #>	--cf_ack
--sequence <sequence #>	--cf_poll
--ssid <ssid string>	--null_data
	--script <file name>

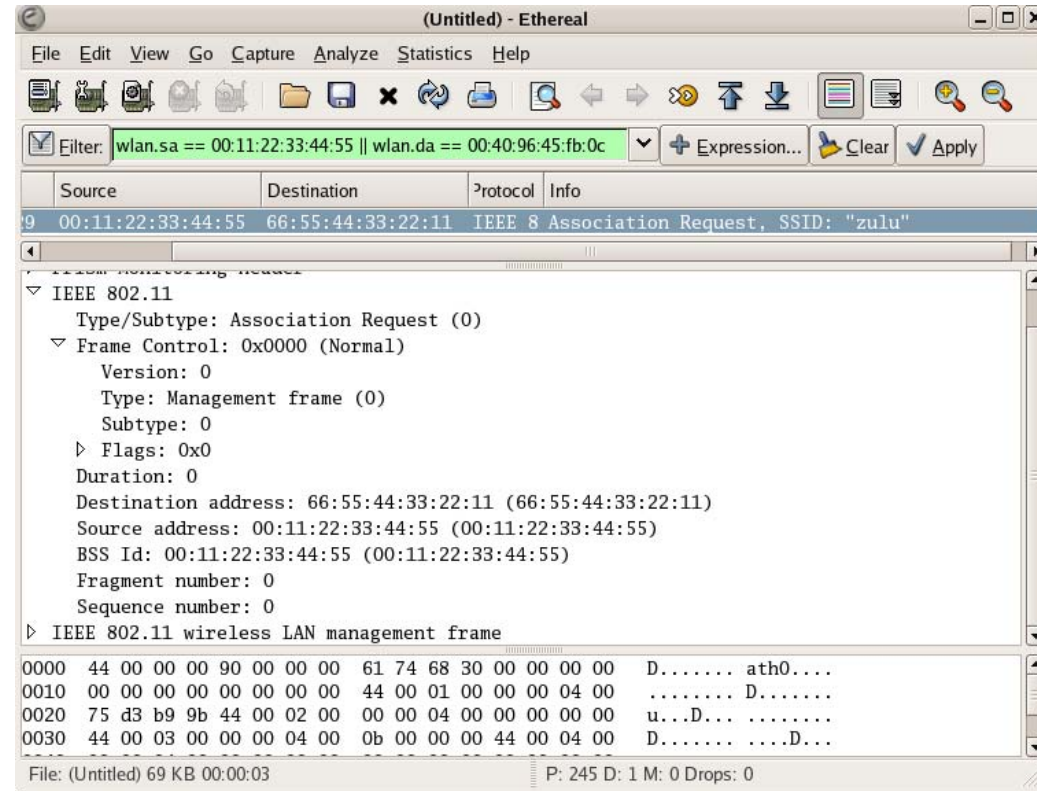


Simple Example of Zulu

```
zulu -i ath0 -t assoc-request
```



```
zulu -i ath0 -t assoc-request -s 001122334455  
-d 665544332211
```



Complex Zulu Example

zulu -i ath0 -t 5

-s 001122334455

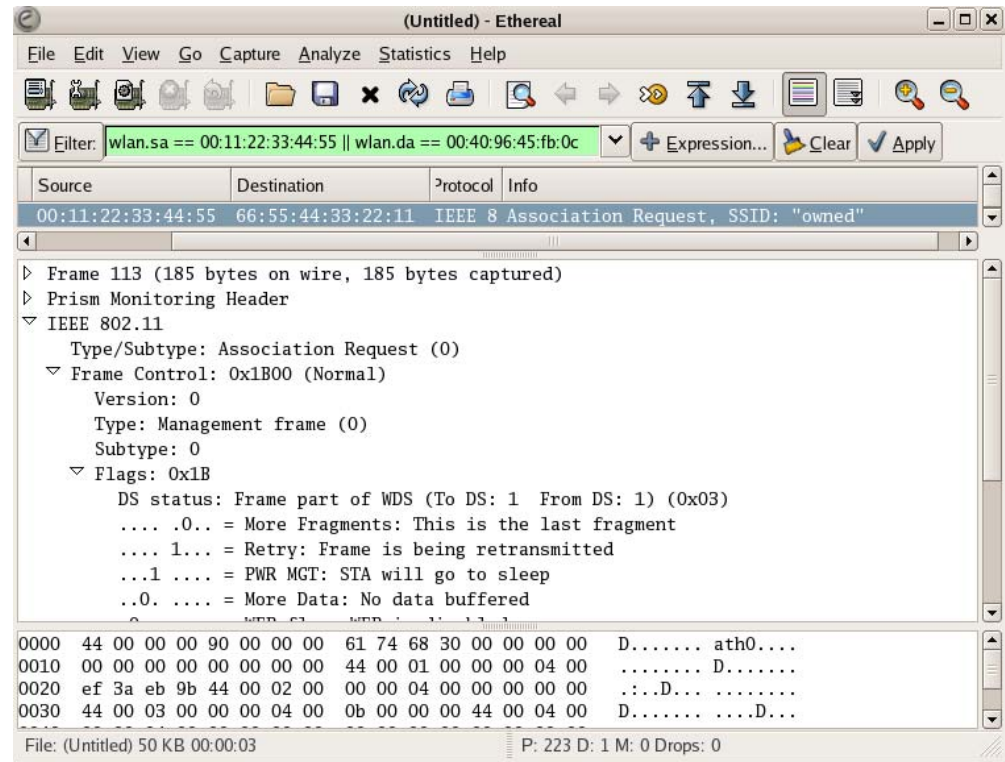
-d 665544332211

-p

--bridge

--sequence 1234

--ssid owned



Scripting in Zulu

```
zulu -i ath0 -file script.txt
```

script.txt

```
DATA 10  
Beacon 20  
RTS 30
```

This script will send out 10 data frames followed by 20 Beacons and 30 RTS frames all with default settings



How is Zulu different from other wireless frame generation tools?

- File2air
 - Lets you inject custom frames, but requires detailed knowledge of the frame structure
- libwlan and libradiate
 - Both are meant as programming libraries to allow programmers to inject wireless frames
- AirJack and FakeAP
 - Limited injection capabilities
- Pcap2air
 - Allows you to inject packets from a pcap file



Future Work

- Support for more wireless device drivers
- Testing of Zulu on more Linux platforms
- Better documentation
- Evaluation of command line options to make it easier to use
- Improved scripting support
- Better integration of lorcon



Where can I get Zulu?

moblog.colorado.edu/zulu



Acknowledgements

Joshwr1ght and Dragorn for writing lorcon
download the full version:

<http://802.11ninja.net/code/lorcon-current.tgz>

Air Defense (www.airdefense.net) and Dr.
Douglas Sicker for employing us while working
on this tool

Kevin Bauer for doing QA

