

Wireshark Developer and User Conference

Using Wireshark with the CloudShark Plug-in

Monday June 25th 2012



Joe McEachern

CEO and Founder | CloudShark



Zach Chadwick

Lead Developer | CloudShark

SHARKFEST '12

UC Berkeley

June 24-27, 2012

WARNING: This presentation may be interactive! Start packet surfing right from your seat!



@cloudshark



<https://surf.cloudshark.org>

User: **sharkfest**

Password: **sharkfest**



Act One: The Evolution of CloudShark

“We’re going to need a bigger boat!”
-- Jaws, 1975

In the Beginning ...

It all started at QA Cafe in Portsmouth, New Hampshire, USA ...



... We develop CDRouter for testing CPE devices
(aka gateways, routers, edge devices).



... Our test software has probably
been used to test the router in your
home.

... Lots of packets, lots of Wireshark



Act One: The CloudShark Story



The CloudShark TimeLine



2010	2011	2012
<ul style="list-style-type: none">• QA Cafe developed technology to view packets in the web• We called it “inline packet decode” Sexy!• We wanted to make this capability available to a wider audience• Launched free CloudShark.org	<ul style="list-style-type: none">• What about security in the cloud?• “Pushing packets to the cloud is a dumb idea!”• Okay, here is the CloudShark appliance. Deploy it in your own network!	<ul style="list-style-type: none">• Still using Wireshark to create captures.• Let’s make it easier to send your capture files from Wireshark to CloudShark• Released a GPL Wireshark plug-in that makes it easier to send captures to CloudShark

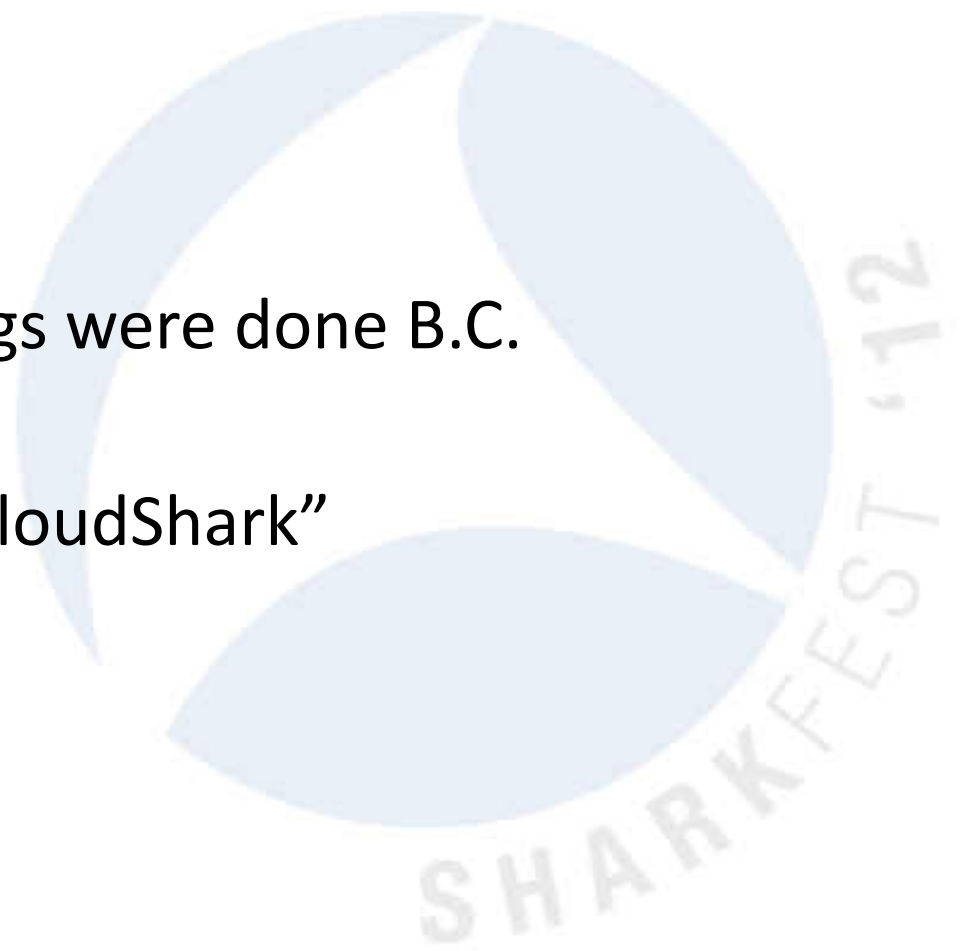


Act Two: Quick Tour of CloudShark

“You got any better suggestions”
-- Jaws, 1975

Why CloudShark?

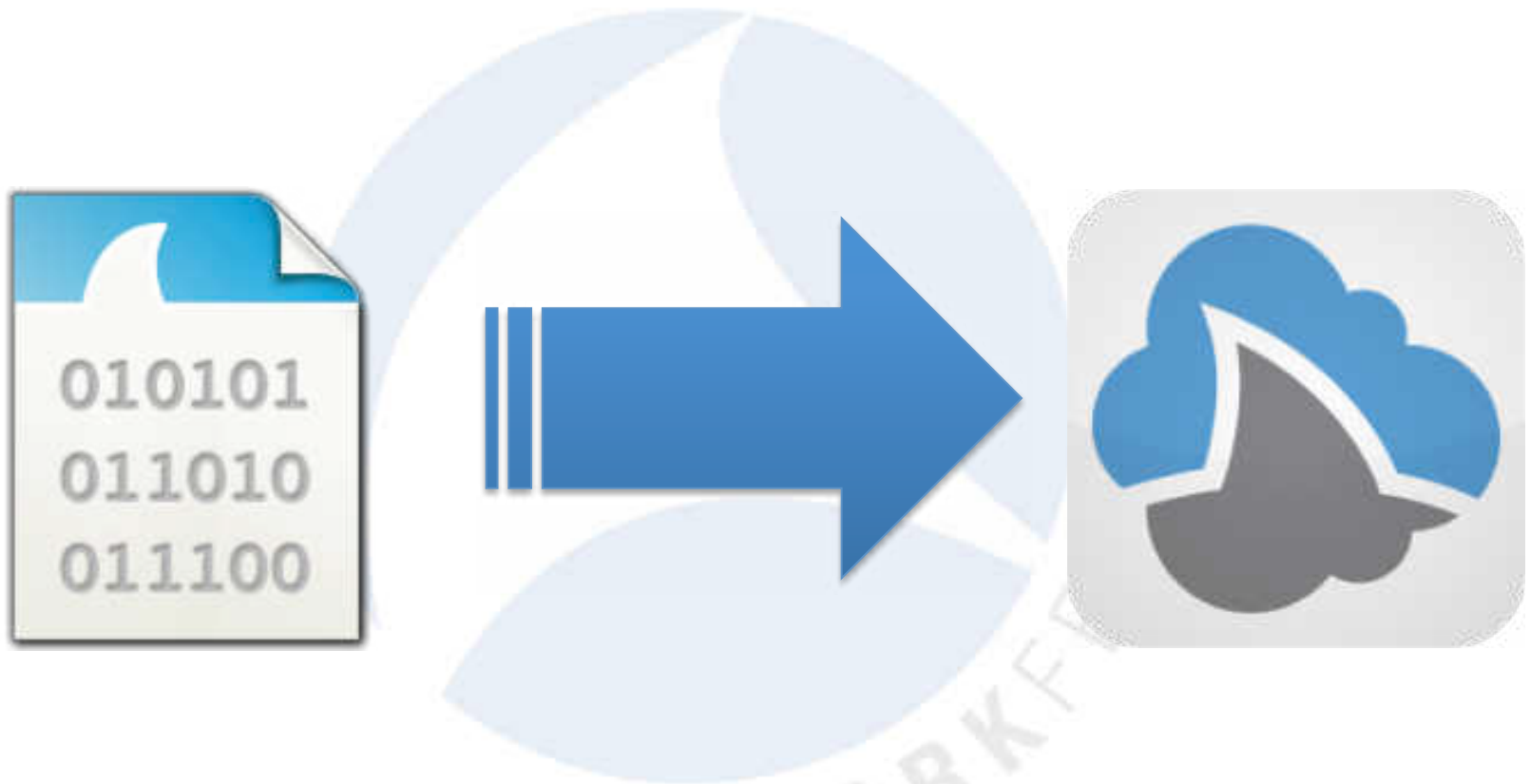
- How things were done B.C.
- “Before CloudShark”



Why CloudShark?

- “Hey can you look at something?”
- Sticky Fingers
- BLT not TCP
- SneakerNet

Why CloudShark?



<https://www.cloudshark.org/captures/f62e1db77ba0>

Why CloudShark?

- Store
- View
- Analyze
- Annotate
- Share



Why CloudShark?

The screenshot displays the CloudShark web interface. On the left, a sidebar shows a list of captured packets, with packet 10 highlighted. The main area is divided into two sections:

- HTTP Traffic from urla.asp:** This section features a line graph showing traffic volume over time. Below the graph, a text box displays the raw packet data for 'Follow Stream 7 in urla.asp'. The data includes an HTTP 200 OK response with headers such as 'Date: Tue, 15 May 2012', 'Expires: Tue, 15 May 2012', 'Cache-Control: private', 'Content-Type: text/javascript', and 'Content-Disposition: inline'. The body of the response contains a JavaScript function definition for 'showStream'. At the bottom of this section, a hex dump of the packet data is visible.
- SIP Call Flow for FAX-Call-138-CA-TDM-SIP-FB-1.pcap:** This section provides a detailed sequence of SIP messages between two endpoints: 136.132.166.101 and 192.168.100.219. The sequence includes:
 - INVITE SDP (g711A G726-32RTPTType-102 telephone-eventRTPType-1)
 - 100 Trying
 - 180 Ringing
 - 200 OK SDP (g711A telephone-eventRTPType-102)
 - ACK
 - INVITE SDP (g711A)

Why CloudShark?

- Centralized storage



Why CloudShark?

The screenshot displays the CloudShark web interface. On the left, there are sections for 'Upload Files' (with a 'Drag & Drop Files Here' area) and 'Import from URL'. Below these is a 'Search for Files' section with a text input field and a dropdown arrow. The main area is a table of capture files with columns for 'Date Added', 'User', 'Group', and 'File Name'. The table contains numerous rows of data, including dates from May to June 2012 and various file names like 'cloudshark-capture-decodes.mka', 'http://www.cloudshark.org/captures/24', and 'winshark-plugin-ia.-BCV-.cap'. On the right side, a 'Search for Files' panel is open, showing a search filter dropdown set to '6/8/2012 - 6/15/2012'. A list of filter options is displayed, including 'Today', 'Last 7 days', 'Month to date', 'Year to date', 'The previous Month', 'Specific Date', 'All Dates Before', 'All Dates After', and 'Date Range'.

Date Added	User	Group	File Name
Today 10:12 AM	admin		cloudshark-capture-decodes.mka
Wed Jun 13, 2012 1:25 PM	admin		http://www.cloudshark.org/captures/24
Thu Jun 07, 2012 11:25 AM	admin		winshark-plugin-ia.-BCV-.cap
Wed Jun 06, 2012 2:00 PM	quest		seahtst.pcap
Wed Jun 06, 2012 1:03 PM	admin		http://cloudshark.org/captures/1011169
Wed Jun 06, 2012 10:32 AM	admin		seahtst.pcap
Wed Jun 06, 2012 10:19 AM	admin		seahtst.pcap
Wed Jun 06, 2012 10:18 AM	admin		seahtst.pcap
Fri Jun 01, 2012 10:36 AM	admin		all_of_them.pcap
Fri Jun 01, 2012 10:28 AM	admin		seahtst.pcap
Fri Jun 01, 2012 10:27 AM	admin		url.cap
Fri Jun 01, 2012 10:27 AM	admin		big_sqli.cap
Fri Jun 01, 2012 10:27 AM	admin		3MBattack.pcap
Fri Jun 01, 2012 10:26 AM	admin		big_sqli.cap
Wed May 30, 2012 10:30 AM	admin		SUPERSET.cap
Wed May 23, 2012 1:25 PM	quest		seahtst.pcap
Wed May 23, 2012 1:07 PM	quest		SUPERSET (1).cap
Wed May 23, 2012 1:06 PM	quest		SUPERSET.cap
Wed May 23, 2012 1:04 PM	quest		problem.pcap
Wed May 23, 2012 1:01 PM	quest		seahtst.pcap
Wed May 23, 2012 12:39 PM	quest		FAX-Cat-09-CA-TDM-SIP-FB-1.pcap
Wed May 23, 2012 12:37 PM	quest		big_sqli.cap
Wed May 23, 2012 12:36 PM	quest		seahtst.pcap
Wed May 23, 2012 11:07 AM	quest		seahtst.pcap
Tue May 15, 2012 12:37 PM	admin		med-data.pcap
Tue May 15, 2012 11:20 AM	admin		url.cap
Sun May 13, 2012 1:22 PM	admin		http://www.cloudshark.org/captures/161
Wed May 02, 2012 3:04 PM	admin		packet.cap
Wed May 02, 2012 3:04 PM	admin		stream4.pcap
Wed May 02, 2012 3:04 PM	admin		truncated.pcap
Wed May 02, 2012 3:04 PM	admin		800teachers.pcap
Wed May 02, 2012 3:04 PM	admin		400teachers.pcap

- Now where did I put that...?
- Indexes the metadata
- Searching

Quick Demo

Start packet surfing right from
your seat!



@cloudshark



<https://surf.cloudshark.org>

User: **sharkfest**

Password: **sharkfest**

Why CloudShark?

- How do we make this even easier?
- It's plugin time!



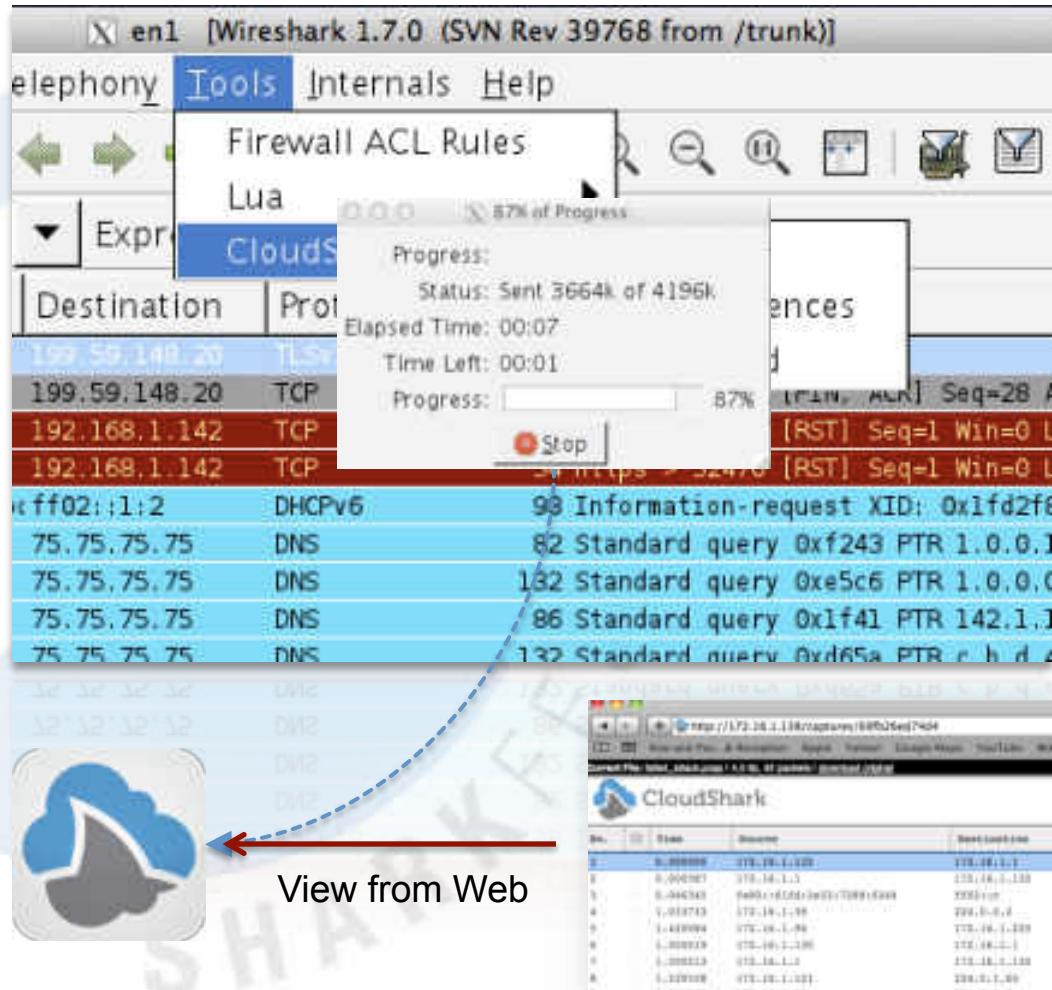


Act Three: Getting Started with the Plugin

“That’s some bad hat Harry”
-- *Jaws*, 1975

Wireshark Plug-in

- The plug-in uses Wireshark's Lua plug-in interface.
- Once installed, the Tools menu is extended with a new CloudShark option.
- Use the Upload option to push the current capture file to CloudShark.
- Wireshark opens the default browser with a CloudShark session URL.



Installation

- Download free installer from cloudshark.org. Latest version is 1.0.1.
- Installers available for Windows, OSX, and generic unix (*.tgz).
- Installed under user's Wireshark plugins directory (platform specific).
- Simply restart Wireshark and plug-in is detected automatically.



Configuration

- Text based configuration available from CloudShark menu
- Configure CloudShark URL to CloudShark.org or your own appliance
- Setup API key, user, password
- Setup additional tags
- Certificate configuration for curl



```
--[[
This is the configuration file for the
CloudShark plugin. Visit
http://appliance.cloudshark.org for
additional help
--]]

-- URL: The CloudShark appliance URL
CLOUDSHARK_URL = "https://www.cloudshark.org"

-- API: The API token to use
CLOUDSHARK_API_KEY = "59f5893a634b99d1bbc2cd9587a5a508"

-- Tags: A comma separated list of tags
CLOUDSHARK_TAGS = ""

-- User: The user name (only if login is required)
CLOUDSHARK_USER = ""

-- Password: The password (only if login is required)
CLOUDSHARK_PASSWORD = ""

-- Tshark: To enable tshark support for the plugin,
-- set the CLOUDSHARK_TSHARK setting to "y" for auto
-- mode or "prompt" for prompting mode.
CLOUDSHARK_TSHARK = "n"

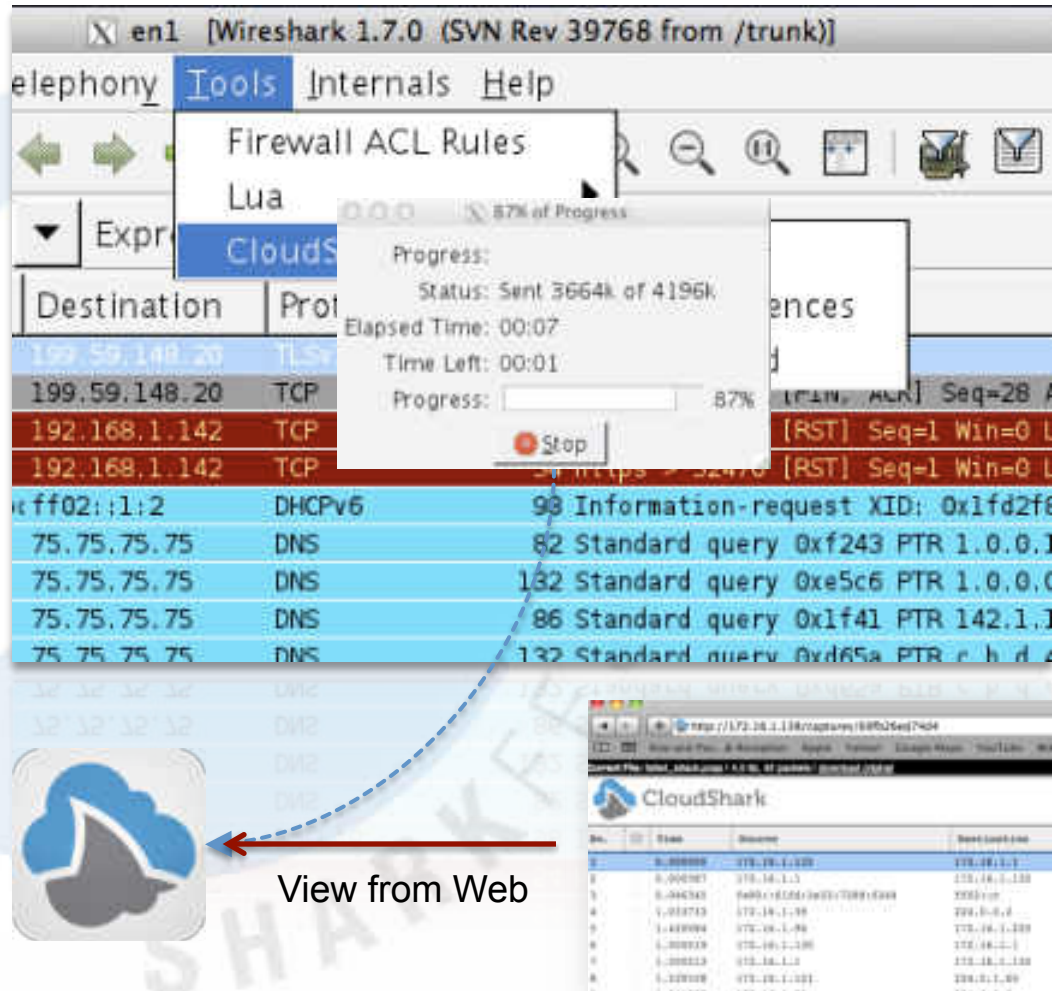
-- Curl: The path to curl if non-standard
-- Paths should be formatted with [[path]]
-- Remove the -- below to uncomment
-- CLOUDSHARK_CURL = [[C:\example\curl.exe]]

-- CA Bundle: The path to an alternative CA bundle file in pem format
-- Paths should be formatted with [[path]]
-- Remove the -- below to uncomment
-- CLOUDSHARK_CABUNDLE = [[C:\example\curl-ca-bundle.crt]]
```

Save Close

Wireshark Plug-in

- Works with live capture or stopped/loaded capture.
- Upload sends capture to CloudShark web API using https POST.
- Plug-in checks response and determines CloudShark session URL.



Live Plug-in Examples

Start surfing now. Sample captures will be uploaded to surf.cloudshark.org.



@cloudshark



<https://surf.cloudshark.org>

User: sharkfest

Password: sharkfest



Act Four: Using the Plug-in with tshark

“This was no boat accident”
-- *Jaws*, 1975

Using the Plug-In with tshark

- User interface challenge
- Off by default
- Can enable automatic uploads or prompting through Cloudshark preferences file
- Great for scripting and automation tools
- CloudShark session URL displayed in tshark output

```
Joe — bash — 79x24
Josephs-MacBook-Pro:~ joe$ tshark -i en1 -c 3
CloudShark plugin for Wireshark (c) 2012
Version 1.0 rev 136
Developed by QA Cafe
Capturing on en1
0.000000 192.168.1.1 -> 239.255.255.250 SSDP 400 NOTIFY * HTTP/1.1
0.003413 192.168.1.1 -> 239.255.255.250 SSDP 337 NOTIFY * HTTP/1.1
0.006595 192.168.1.1 -> 239.255.255.250 SSDP 328 NOTIFY * HTTP/1.1
3 packets captured

Uploading capture file to CloudShark via https://www.cloudshark.org
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload    Total   Spent    Left   Speed
100 1531    0   66 100 1465    58 1295  0:00:01  0:00:01  --:--:-- 1513

HTTP Response Code: 200
A new CloudShark session has been created at:

https://www.cloudshark.org/captures/c3be7b05fc17

Josephs-MacBook-Pro:~ joe$
Josephs-MacBook-Pro:~ joe$
Josephs-MacBook-Pro:~ joe$
Josephs-MacBook-Pro:~ joe$
```

Live Tshark Examples

Here come some more waves.
Grab your board and head to
surf.cloudshark.org.



@cloudshark



<https://surf.cloudshark.org>

User: sharkfest

Password: sharkfest



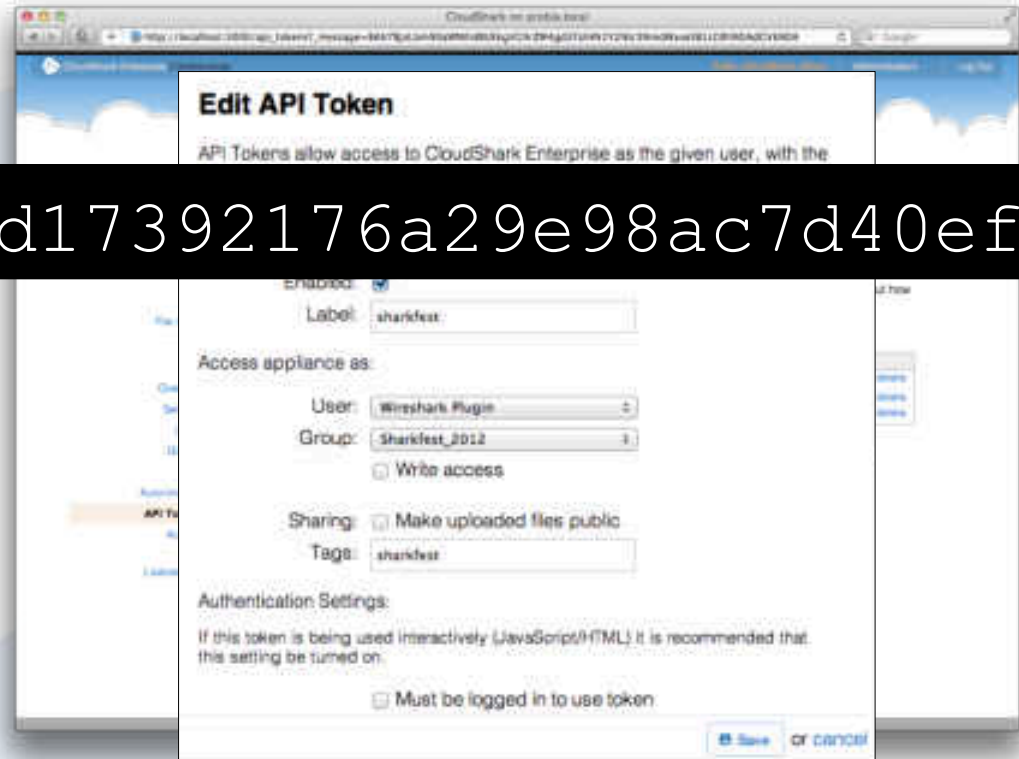
Act Five: Setting up for the Plug-in

“Come on into the water.”
-- *Jaws*, 1975

Setting up for the Plugin

1. Create Token
2. Settings
3. Copy/Paste

d02fd17392176a29e98ac7d40ef17c



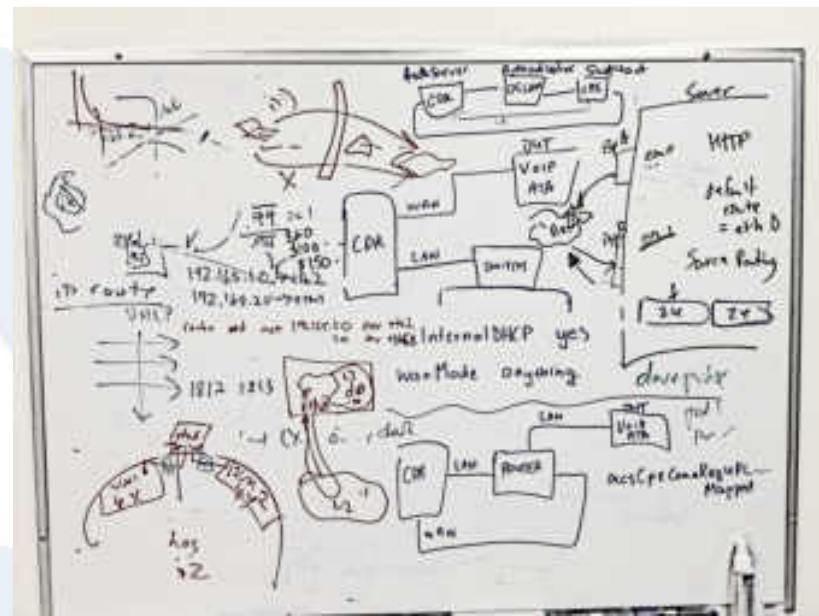


Act Six: A quick look under the hood

This shark, swallow you whole.
-- *Jaws*, 1975

A Look Under the Hood

- Lua provides cross platform support
- How do you get Wireshark to speak web? Use combination of Curl and Lua JSON library.
- Not many Wireshark GUI controls available through Lua – but enough!
- Support tshark by detecting GUI.
- Go deeper in Wednesday's Sharkfest session.





Act Seven: Lessons Learned

What we have here is a eating machine.
-- Jaws, 1975

Lessons Learned: Uploads

- No signups
- No logins
- No limit to imagination
of uploads!



Lessons Learned: Uploads

- MP3
- MPEG
- JPEG
- Historical reasons for support?

Lessons Learned: Uploads

- Exploits
- Denial Of Service
- Sandbox



Lessons Learned: Mobile

- “Out of the office”



*standard data and messaging rates may apply

Lessons Learned: Data Size

- Bandwidth issues
- Too much data
- Information without all the data
- Caching

Lessons Learned: Community

- Great community
- PacketLife.org
- ask.wireshark.org
- SharkFest!



Act Eight: Wrapping up

Any special questions?
-- Jaws, 1975

Wrapping up

- Learn to packet surf today! Download the plugin now from cloudshark.org
- Login to <https://surf.cloudshark.org>
`user: sharkfest`
`password: sharkfest`
- Try out our capture challenge for Sharkfest attendees!
<http://bit.ly/sharkfest-2012>
- Come back for Wednesday's 11:00 session
"Using Lua to implement the Wireshark Plug-in"

Have a great Sharkfest!

