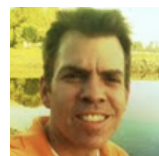


Wireshark Developer and User Conference

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

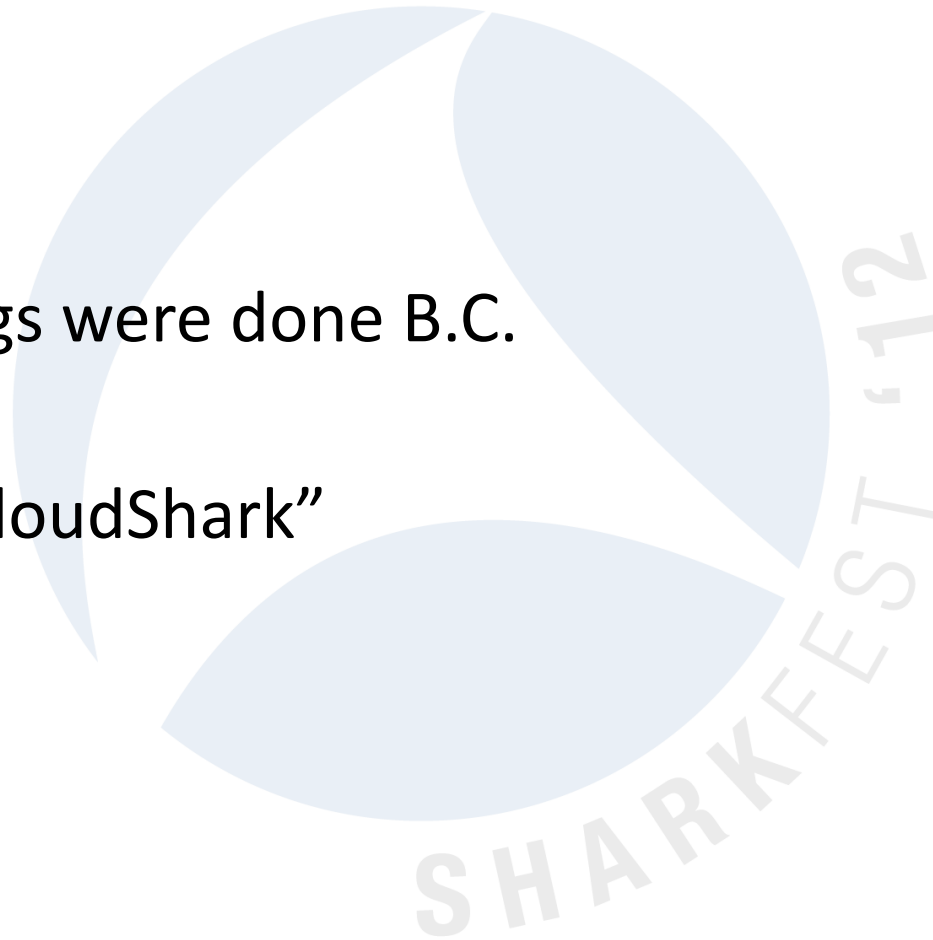


Act Two: Quick Tour of CloudShark

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

Why CloudShark?

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

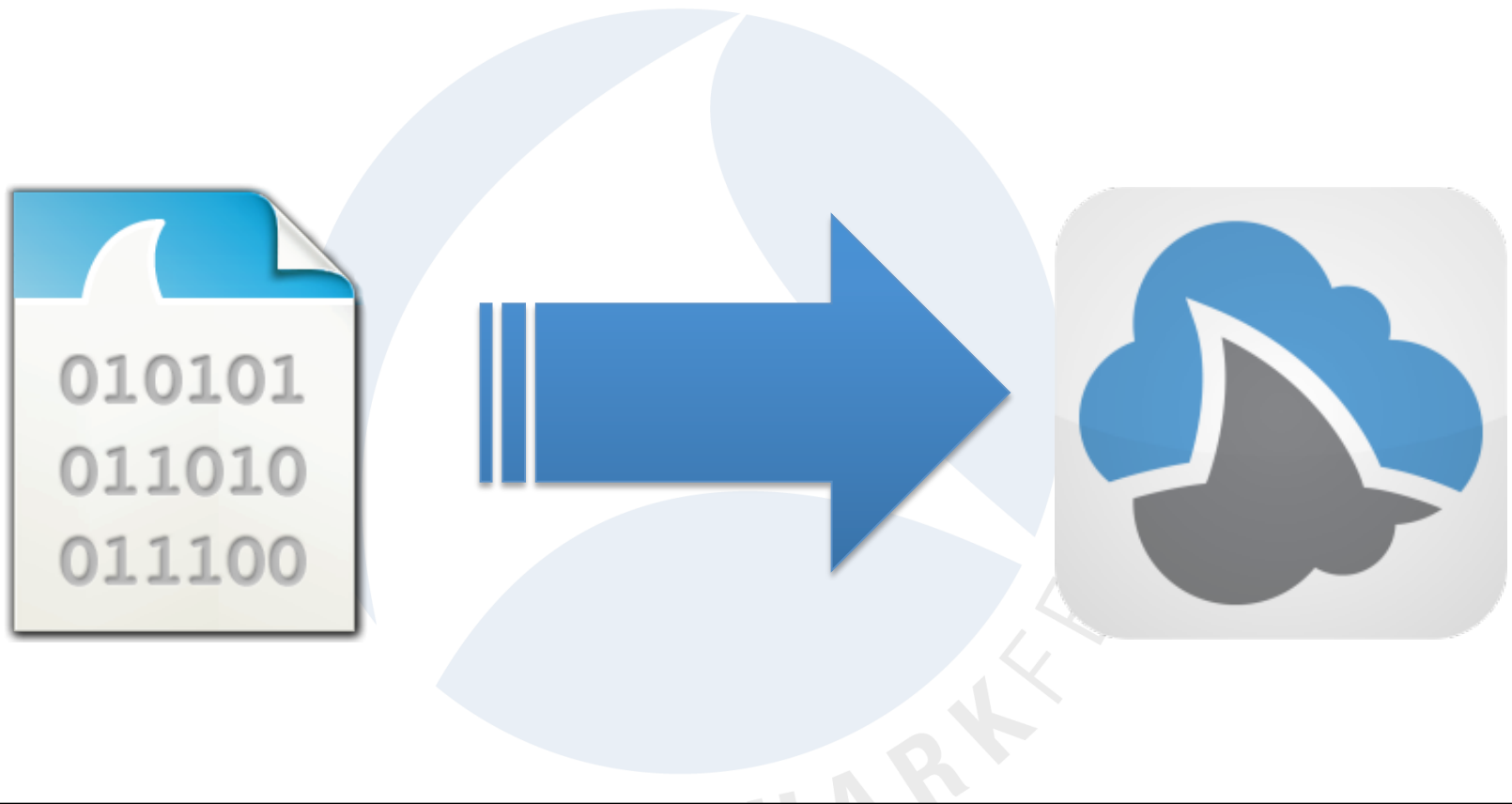


Why CloudShark?

- “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 file list shows 'urls.cap' selected. The main area is titled 'HTTP Traffic from urls.cap' and features a line graph showing traffic volume over time. A 'Follow Stream 7' window is open, displaying a detailed view of an HTTP 200 OK response, including headers like 'Date: Tue, 15 May 2012' and 'Content-Type: text/javascript'. Below the headers is a hex dump of the packet data. To the right, a 'SIP Call Flow for FAX-Call-t38-CA-TDM-SIP-FB-1.pcap' window shows a sequence of SIP messages between IP addresses 138.132.169.101 and 192.168.100.219. The messages include INVITE SDP, 100 Trying, 180 Ringing, 200 OK SDP, ACK, and INVITE SDP (g711A). A 'SIP From' field is highlighted with the value '<sip:unavailable@hostportion>'. At the bottom right, there are buttons for 'Open in new window' and 'Done'.

Why CloudShark?

- Centralized storage



SHARKFEST

Why CloudShark?

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

The screenshot shows the CloudShark web interface. The main content area displays a table of capture files with columns for Date Added, User, Group, and File Name. The table lists various capture files, including 'cloudshark-custom-decodes.m4v', 'wireshark-plugin-lua_nBCPvf.cap', and 'all_of_them.pcap'. On the right side, there is a 'Search for Files' panel with a search filter dropdown and a date range selector. The date range selector is open, showing options like 'Today', 'Last 7 days', 'Month to date', 'Year to date', 'The previous Month', 'Specific Date', 'All Dates Before', 'All Dates After', and 'Date Range'. The date range is currently set to '6/8/2012 - 6/15/2012'.

Date Added	User	Group	File Name
Today 10:12 AM	admin		cloudshark-custom-decodes.m4v
Wed Jun 13, 2012 1:05 PM	admin		https://www.cloudshark.org/captures/3k
Thu Jun 07, 2012 11:25 AM	admin		wireshark-plugin-lua_nBCPvf.cap
Wed Jun 06, 2012 2:29 PM	guest		localhost.pcap
Wed Jun 06, 2012 1:53 PM	admin		http://cloudshark.org/captures/701519d
Wed Jun 06, 2012 10:32 AM	admin		http://cloudshark.org/captures/5a38164375fc-953c-90ac0007ef
Tue Jun 05, 2012 12:49 PM	admin		http://cloudshark.org/captures/196a079a55
Tue Jun 05, 2012 12:35 PM	admin		http://cloudshark.org/captures/196a079a55
Fri Jun 01, 2012 10:38 AM	admin		all_of_them.pcap
Fri Jun 01, 2012 10:38 AM	admin		localhost.pcap
Fri Jun 01, 2012 10:27 AM	admin		urls.cap
Fri Jun 01, 2012 10:27 AM	admin		big_sip2.cap
Fri Jun 01, 2012 10:27 AM	admin		SMBAttack.pcap
Fri Jun 01, 2012 10:26 AM	admin		big_sip2.cap
Wed May 23, 2012 1:44 PM	guest		SUPERSET.cap
Wed May 23, 2012 1:41 PM	guest		SUPERSET (1).cap
Wed May 23, 2012 1:38 PM	guest		zeus-sample-3.pcap
Wed May 23, 2012 1:07 PM	guest		SUPERSET (1).cap
Wed May 23, 2012 1:06 PM	guest		SUPERSET.cap
Wed May 23, 2012 1:04 PM	guest		probie-slow.cap
Wed May 23, 2012 1:01 PM	guest		localhost.pcap
Wed May 23, 2012 12:39 PM	guest		FAX-Call-438-CA-TDM-SIP-FB-1.pcap
Wed May 23, 2012 12:37 PM	guest		big_sip2.cap
Wed May 23, 2012 12:35 PM	guest		localhost.pcap
Wed May 23, 2012 11:02 AM	guest		localhost.pcap
Tue May 15, 2012 12:37 PM	admin		med-data.pcap
Tue May 15, 2012 11:20 AM	admin		urls.cap
Sun May 13, 2012 1:22 PM	admin		https://www.cloudshark.org/captures/a1
Wed May 02, 2012 3:04 PM	admin		1packet.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		8000packets.pcap
Wed May 02, 2012 3:04 PM	admin		499packets.pcap

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.

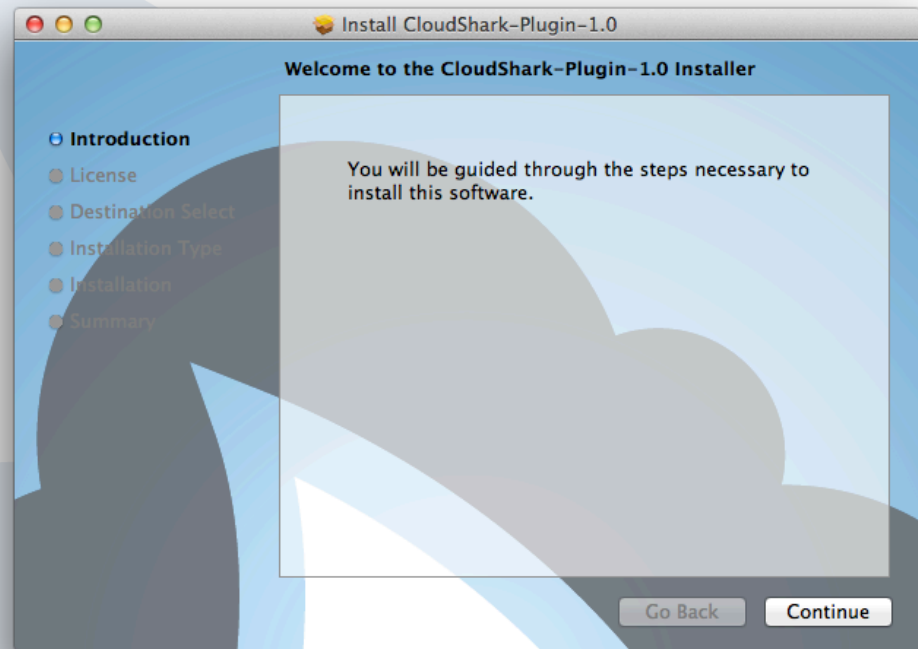
The screenshot shows the Wireshark 1.7.0 interface. The Tools menu is open, showing the CloudShark option. A progress dialog box is displayed over the packet list, showing the upload status: "Progress: 87%", "Status: Sent 3664k of 4196k", "Elapsed Time: 00:07", and "Time Left: 00:01". A "Stop" button is visible in the dialog. Below the dialog, a browser window is open, displaying the CloudShark web interface. The browser address bar shows the URL: <http://172.16.1.138/captures/69fb26ed74d4>. The browser title is "CloudShark". The current file is "failed_attack.pcap | 4.5 kb, 42 packets | download original". The browser displays a table of captured packets:

No.	Time	Source	Destination
1	0.000000	172.16.1.135	172.16.1.1
2	0.000387	172.16.1.1	172.16.1.135
3	0.046345	fe80::61fd:3e32:7288:f244	ff02::c
4	1.033733	172.16.1.39	224.0.0.2
5	1.420084	172.16.1.96	172.16.1.255
6	1.500019	172.16.1.135	172.16.1.1
7	1.500213	172.16.1.1	172.16.1.135
8	1.539108	172.16.1.121	224.0.1.60

A red arrow points from the CloudShark logo in the bottom left corner to the browser window, with the text "View from Web" next to it.

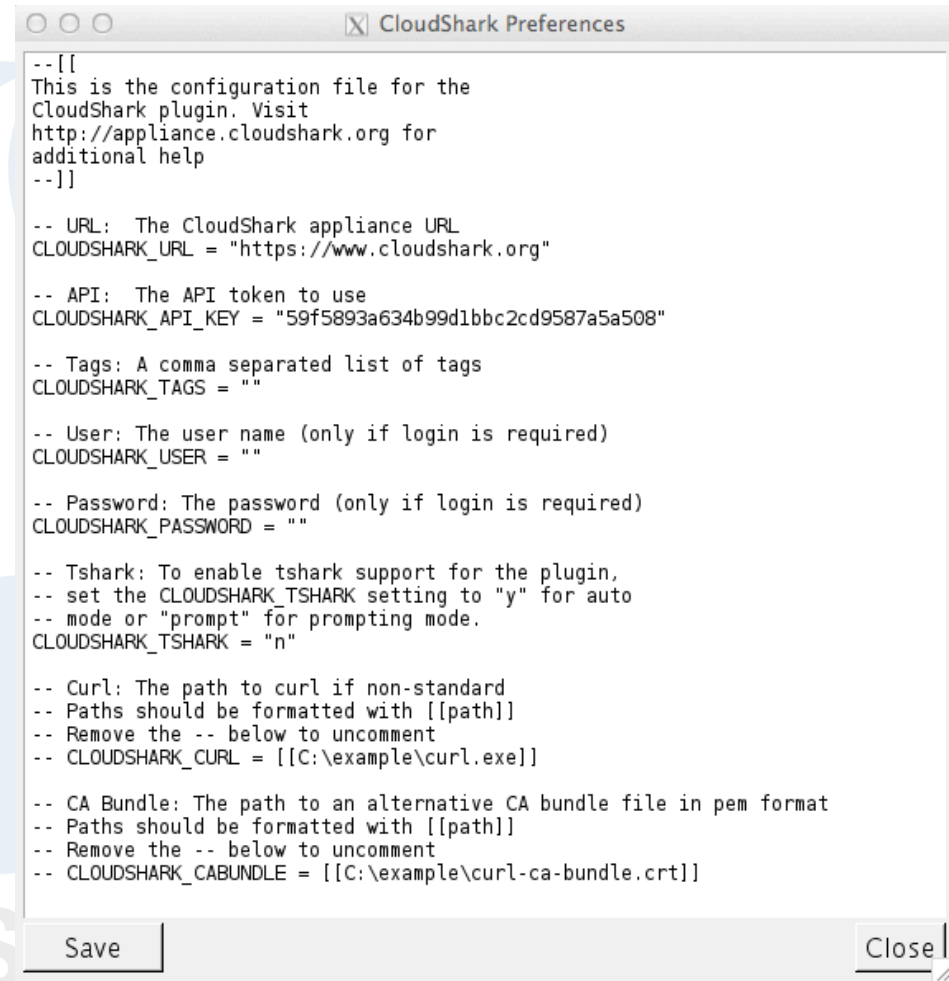
Installation

- 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.

The screenshot shows the Wireshark 1.7.0 interface with a 'CloudShark' progress dialog box. The dialog indicates that 3664k of 4196k has been sent, with 00:07 elapsed time and 00:01 time left. A 'Stop' button is visible. Below the dialog, a table of network packets is visible, including TCP, DHCPv6, and DNS packets. At the bottom, a CloudShark logo is shown with a red arrow pointing to it and the text 'View from Web'.

No.	Time	Source	Destination
1	0.000000	172.16.1.135	172.16.1.1
2	0.000387	172.16.1.1	172.16.1.135
3	0.046345	fe80::61fd:3e32:7288:f244	ff02::c
4	1.033733	172.16.1.39	224.0.0.2
5	1.420084	172.16.1.96	172.16.1.255
6	1.500019	172.16.1.135	172.16.1.1
7	1.500213	172.16.1.1	172.16.1.135
8	1.539108	172.16.1.121	224.0.1.60

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

```
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

CloudShark on probe.local

http://localhost:3000/api_tokens?_message=Bah78joLbm90aWNllid8UEkgVG9rZW4gd2FziHN1Y2Nic3NmdWxseS81cGRh%0AdGVk%0A

CloudShark Enterprise / probe.local

Edit API Token

API Tokens allow access to CloudShark Enterprise as the given user, with the

d02fd17392176a29e98ac7d40ef17c

Enabled:

Label:

Access appliance as:

User:

Group:

Write access

Sharing: Make uploaded files public

Tags:

Authentication Settings:

If this token is being used interactively (JavaScript/HTML) it is recommended that this setting be turned on.

Must be logged in to use token

or

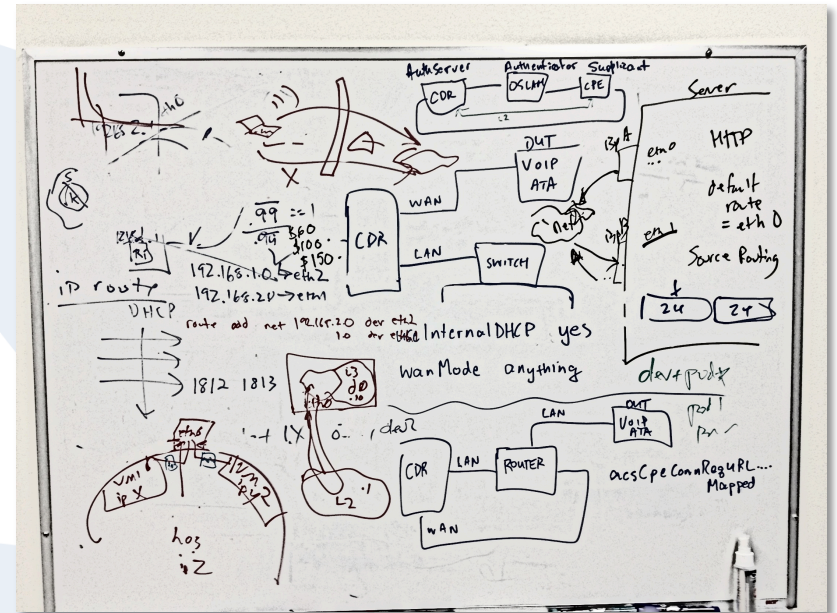


Act Six: A quick look under the hood

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!

