root@glider : whoami

Maverick

Hacker, Ninja
FOSS advocate,
0xn00b Python programmer,
Hack In The Box Crew
Fedora Project Ambassador

@mavjs

root@glider : cat agenda.txt

HTML vs. Plaintext emails

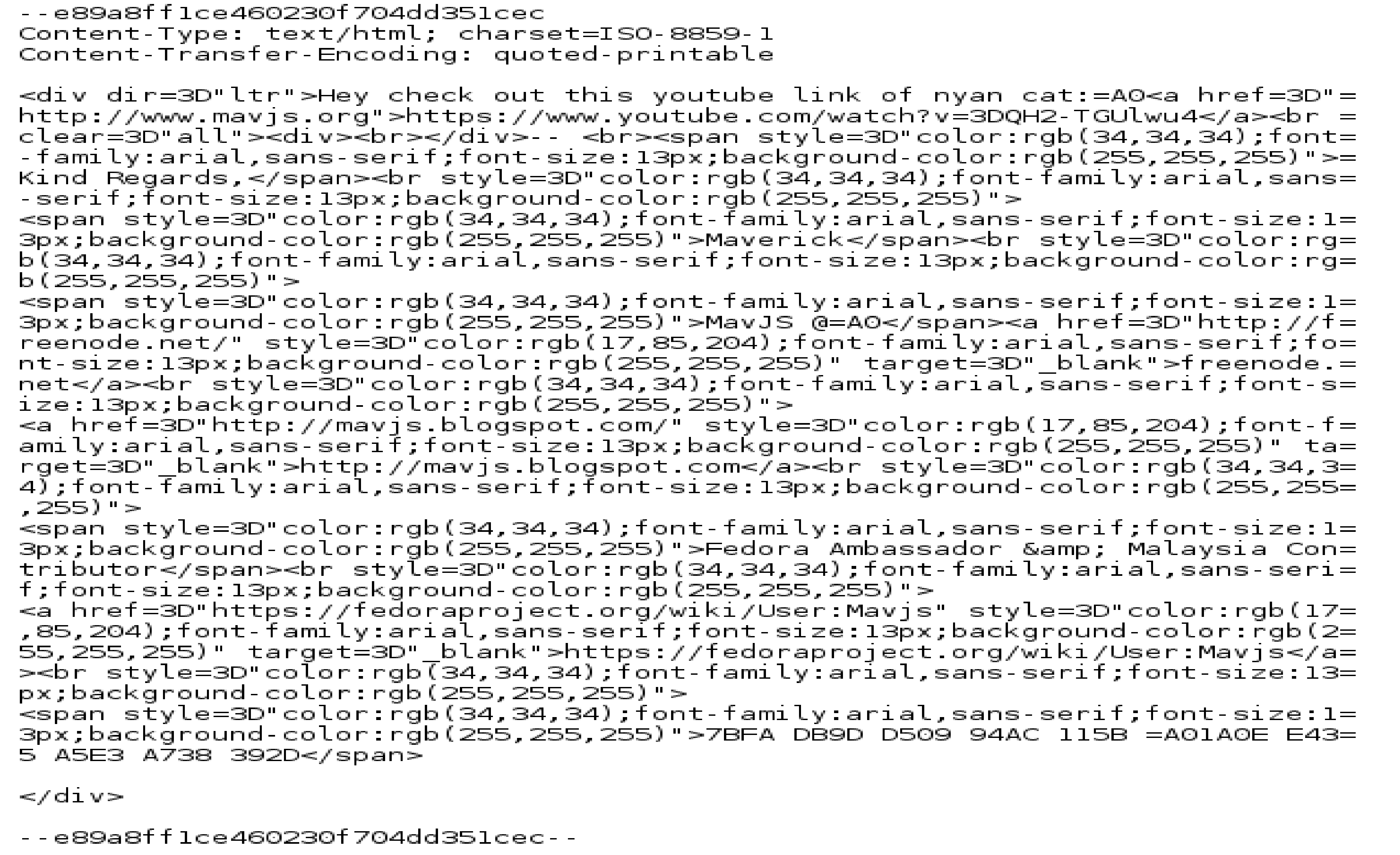
URL expansion

Polipo + Tor to analyse suspicious webpages

root@glider : cat html-plaintext.txt

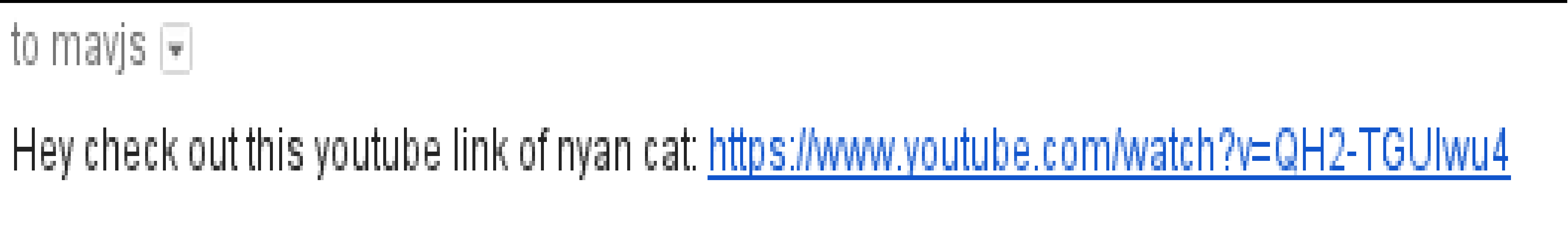
7 reasons why HTML e-mail is EVIL!!! - http://goo.gl/6iVoZ

root@glider : cat html-email.txt



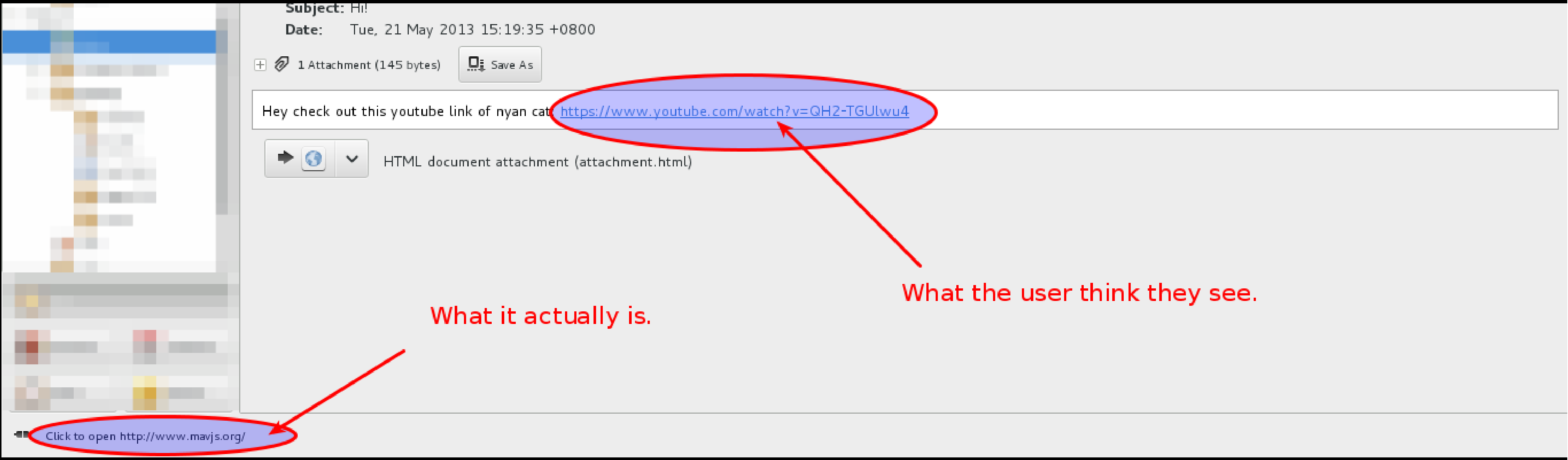
```
--e89a8ff1ce460230f704dd351cec
Content-Type: text/html; charset=ISO-8859-1
Content-Transfer-Encoding: quoted-printable

<div dir=3D"ltr">Hey check out this youtube link of nyan cat:=A0<a href=3D"=
http://www.mavjs.org">https://www.youtube.com/watch?v=3DQH2-TGUlwu4</a><br =
clear=3D"all"><div><br></div>-- <br><span style=3D"color:rgb(34,34,34);font=
-family:arial,sans-serif;font-size:13px;background-color:rgb(255,255,255)">=
Kind Regards,</span><br style=3D"color:rgb(34,34,34);font-family:arial,sans=
-serif;font-size:13px;background-color:rgb(255,255,255)">
<span style=3D"color:rgb(34,34,34);font-family:arial,sans-serif;font-size:1=
3px;background-color:rgb(255,255,255)">Maverick</span><br style=3D"color:rg=
b(34,34,34);font-family:arial,sans-serif;font-size:13px;background-color:rg=
b(255,255,255)">
<span style=3D"color:rgb(34,34,34);font-family:arial,sans-serif;font-size:1=
3px;background-color:rgb(255,255,255)">MavJS @=A0</span><a href=3D"http://f=
reenode.net/" style=3D"color:rgb(17,85,204);font-family:arial,sans-serif;fo=
nt-size:13px;background-color:rgb(255,255,255)" target=3D"_blank">freenode.=
net</a><br style=3D"color:rgb(34,34,34);font-family:arial,sans-serif;font-s=
ize:13px;background-color:rgb(255,255,255)">
<a href=3D"http://mavjs.blogspot.com/" style=3D"color:rgb(17,85,204);font-f=
amily:arial,sans-serif;font-size:13px;background-color:rgb(255,255,255)" ta=
rget=3D"_blank">http://mavjs.blogspot.com</a><br style=3D"color:rgb(34,34,3=
4);font-family:arial,sans-serif;font-size:13px;background-color:rgb(255,255=
,255)">
<span style=3D"color:rgb(34,34,34);font-family:arial,sans-serif;font-size:1=
3px;background-color:rgb(255,255,255)">Fedora Ambassador &amp; Malaysia Con=
tributor</span><br style=3D"color:rgb(34,34,34);font-family:arial,sans-seri=
f;font-size:13px;background-color:rgb(255,255,255)">
<a href=3D"https://fedoraproject.org/wiki/User:Mavjs" style=3D"color:rgb(17=
,85,204);font-family:arial,sans-serif;font-size:13px;background-color:rgb(2=
55,255,255)" target=3D"_blank">https://fedoraproject.org/wiki/User:Mavjs</a=
><br style=3D"color:rgb(34,34,34);font-family:arial,sans-serif;font-size:13=
px;background-color:rgb(255,255,255)">
<span style=3D"color:rgb(34,34,34);font-family:arial,sans-serif;font-size:1=
3px;background-color:rgb(255,255,255)">7BFA DB9D D509 94AC 115B =A01A0E E43=
5 A5E3 A738 392D</span>

</div>

--e89a8ff1ce460230f704dd351cec--
```

root@glider : cat html-email.txt



to mavjs ▾

Hey check out this youtube link of nyan cat: https://www.youtube.com/watch?v=QH2-TGUlwu4



Subject: Hi!

Date: Tue, 21 May 2013 15:19:35 +0800

1 Attachment (145 bytes)

Hey check out this youtube link of nyan cat: https://www.youtube.com/watch?v=QH2-TGUlwu4

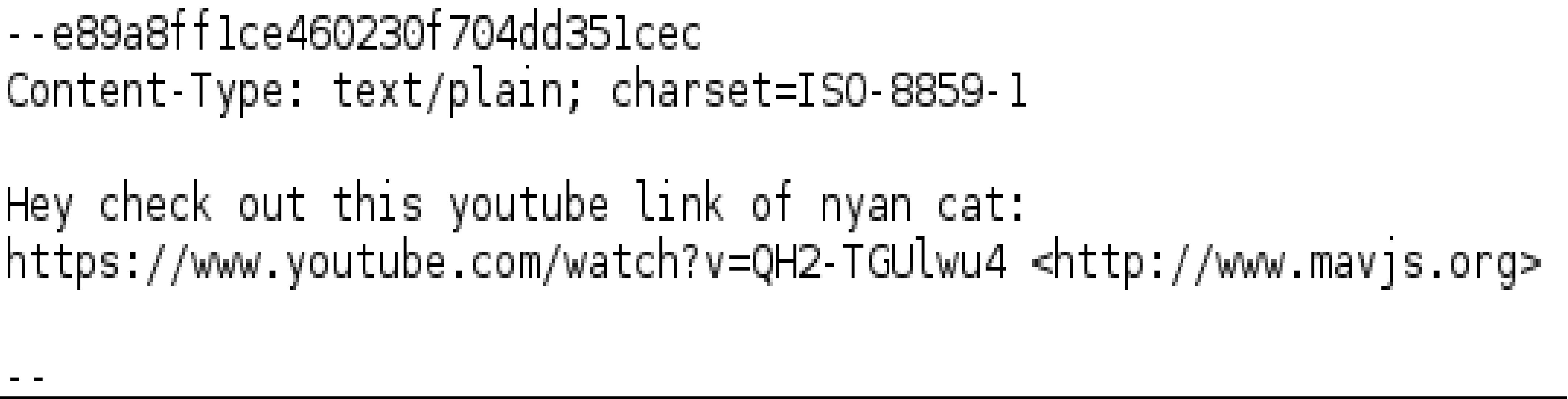
HTML document attachment (attachment.html)

Click to open http://www.mavjs.org/

What the user think they see.

What it actually is.

root@glider : cat plaintxt-email.txt



```
--e89a8ff1ce460230f704dd351cec
Content-Type: text/plain; charset=ISO-8859-1

Hey check out this youtube link of nyan cat:
https://www.youtube.com/watch?v=QH2-TGUlwu4 <http://www.mavjs.org>


--
```

root@glider : cat url-expansion.txt

Inspired from

Use wget(1) To Expand Shortened URLs - http://goo.gl/6qCSz

root@glider : cat url-expansion.txt

Code:

```
wget --max-redirect=0 -O - http://t.co/LDWqmtDM
Location: http://is.gd/jAdSZ3 [following]
0 redirections exceeded.

wget --max-redirect=1 -O - http://t.co/LDWqmtDM
Location:
https://wiki.ubuntu.com/UbuntuOpenWeek
[following]
1 redirections exceeded.
```

root@glider : cat shell-func.txt

```
function surl() {
    if [ "$#" -ne 2 ];
    then
        echo "Error: url not supplied."
        echo "Usage: $0  \"redirect times\" \"url\""
        exit 1
    fi
    wget --max-redirect=$1 $2 | grep -v "Location"
}
```

root@glider : cat install-polipo-tor.txt

```
sudo apt-get install polipo tor

cd /etc/polipo/config
```

E.g. Config:
http://www.andrehonsberg.com/media/polipo.conf

root@glider : cat start-polipo-tor.txt

```
sudo service tor start

sudo service polipo start

Or

sudo /etc/init.d/polipo start
```

root@glider : cat config-wgetrc.txt

e.g. Config: http://goo.gl/KrEOD

e.g. Wgetrc commands: http://goo.gl/mgcF1

```
http_proxy = http://localhost:<polipo port>
use_proxy = on
robots = on
wait = 30
cookies = on
```

```
root@glider : cat test-wget.txt
```

```
wget -O -  http://ifconfig.me/ip

wget -O - http://ifconfig.me/ua
```

root@glider : cat online-tools.txt

https://www.virustotal.com/en/#url

http://urlquery.net/

http://www.mywot.com/

root@glider : cat things-to-do.txt

Don't Click S**T!

Don't let JavaScript run on-demand.