



Free File Uploaders (FFU)

13 August 2009

DERIVED FROM: NSA/CSSM 1-52



Agenda

- Overview of how FFU's work and what the raw data looks like in XKS
- Targets use of FFU's
- How to exploit in XKS
 - HTTP Activity Search
 - (new) Web File Transfer Search



What is an FFU?

- A free file uploader is a website that allows you to upload a file and then hosts that file for others to download.
- Think of the “dropbox” service that we have on NSAnet.
- Since Free File Uploaders are web-based, the HTTP Activity plug-in will be the first place to look for activity
- We’ll also introduce the Web File Transfer plug-in



“Free” part of FFU

- Most FFU sites are free and don't require accounts, but only allow for basic service
- For example, files might only be stored for a short period of time
- Or the person who uploads it does not have a lot of access into who has downloaded their files and how many times



“Premium” accounts for FFU

- Some FFU sites allow for “premium” access, maybe just by registering or maybe by charging the user a fee
- Premium access might allow for more uploads per account, or files that can be stored longer
- Some premium accounts give the uploader “admin” insight into how many times a given file was downloaded (commonly referred to as a “counter”).
- Some premium account sites will even allow the uploader to see the IP address and datetimes associated with each download.



Example of "Premium" access

For Zshare.com:

Maximum upload size 500MB.

Now up to 2GB for [Premium users!](#) and 1GB for [registered users!](#)

Privacy: Share your file with the world (Recommended)
 For your eyes only (Private) * [Registered users](#) only



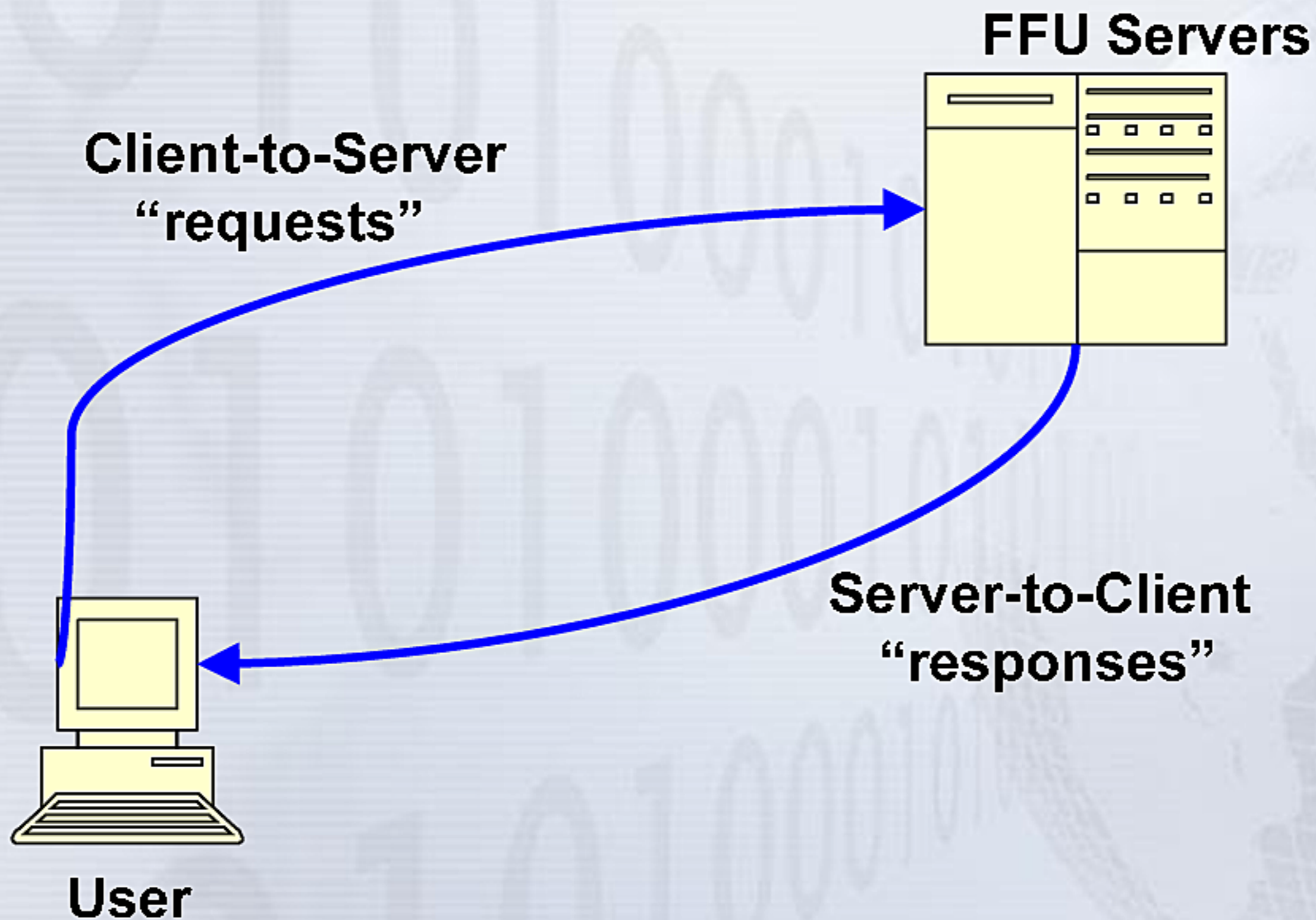
Challenges with FFU

- Almost no FFU activity contains strong selectors (Username or E-mail Addresses) making it difficult to identify our target's use of these services
- In most cases we see a URL to the file that doesn't contain the original filename (eg: <http://www.zshare.net/download/6365962739d34eba>)



HTTP Activity

- HTTP activity comes in two types:





How FFU's work

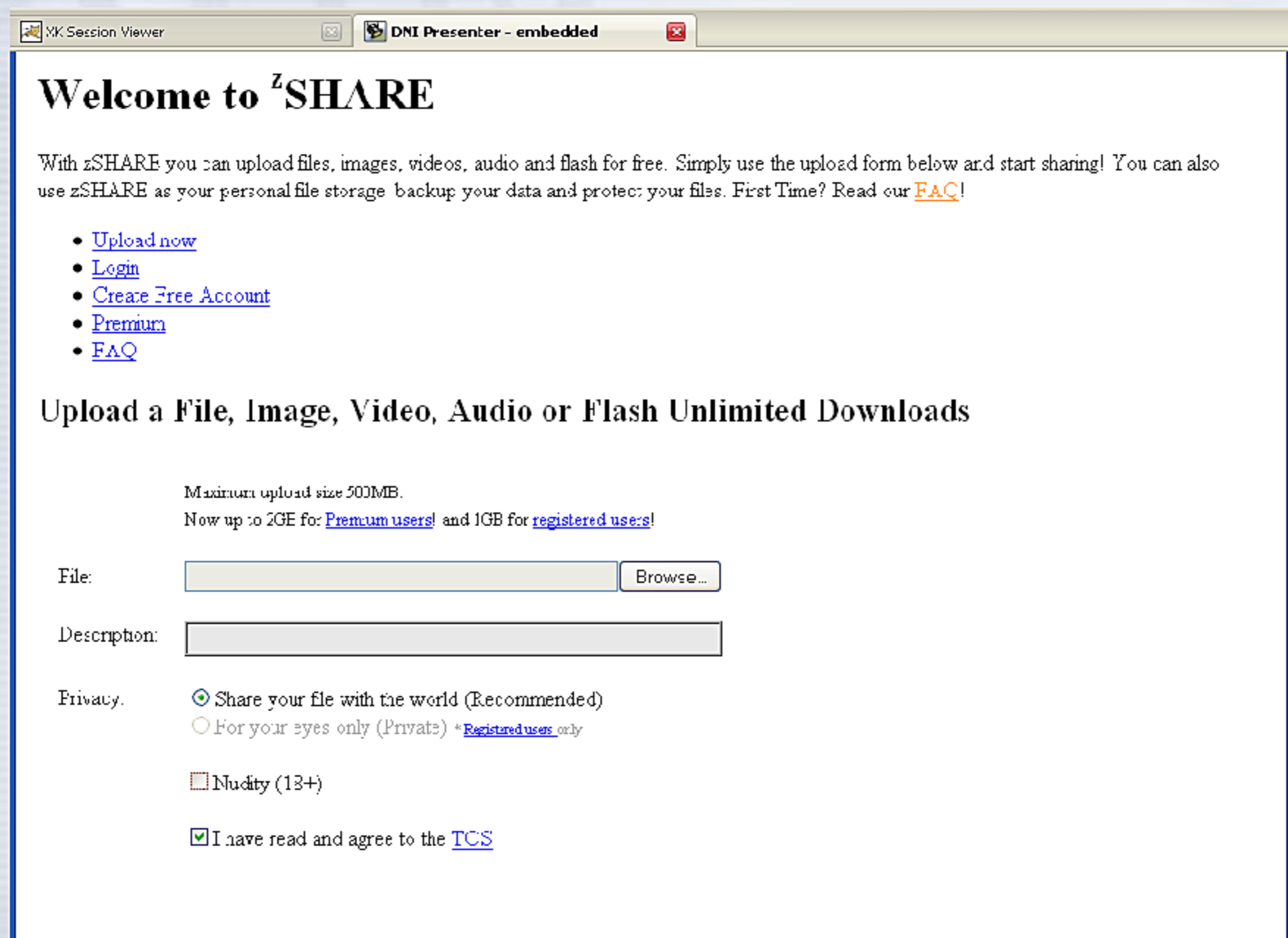
- Client-to-Server request of the homepage

GET / HTTP/1.1	
User-Agent:	Opera/9.22 (Windows NT 5.1; U; en)
Host:	www.zshare.net
Accept:	text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language:	en-US,en;q=0.9
Accept-Charset:	iso-8859-1, utf-8, utf-16, *,q=0.1
Accept-Encoding:	deflate, gzip, x-gzip, identity, *,q=0
Cache-Control:	max-stale=0
Connection:	close
X-BlueCoat-Via:	0A6F53530F3F63EE



How FFU's work

- Server-to-client response of the homepage

A screenshot of a web browser window showing the zSHARE homepage. The browser tabs include "VK Session Viewer" and "DNI Presenter - embedded". The page content includes a welcome message, a list of links (Upload now, Login, Create Free Account, Premium, FAQ), and an upload form with fields for File, Description, and Privacy, along with a checkbox for agreeing to the TCS.

YK Session Viewer DNI Presenter - embedded

Welcome to ^zSHARE

With zSHARE you can upload files, images, videos, audio and flash for free. Simply use the upload form below and start sharing! You can also use zSHARE as your personal file storage backup your data and protect your files. First Time? Read our [FAQ!](#)

- [Upload now](#)
- [Login](#)
- [Create Free Account](#)
- [Premium](#)
- [FAQ](#)

Upload a File, Image, Video, Audio or Flash Unlimited Downloads

Maximum upload size 500MB.
Now up to 2GB for [Premium users!](#) and 1GB for [registered users!](#)

File:

Description:

Privacy: Share your file with the world (Recommended)
 For your eyes only (Private) *[Registered users only](#)

Nudity (13+)

I have read and agree to the [TCS](#)



How FFU's work

■ Client-to-Server POST of the file

```
POST /cgi-bin/ubr_upload.pl?upload_id=6963384d1a981de0b38312900b149ae9
&multiple=0&is_private=0&is_eighteen=0&pass=&descr= HTTP/1.1
User-Agent: Opera/9.22 (Windows NT 5.1; U; en)
Host: dl081.zshare.net:3000
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg,
image/gif, image/x-bitmap, */*;q=0.1
Accept-Language: en-US,en;q=0.9 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Expect: 100-continue
Referer: http://www.zshare.net/
Cookie: sid=65985202ca9ff4f0fd000e0e4a182d59
Cookie2: $Version=1 Connection: Keep-Alive, TE TE: deflate, gzip, chunked, identity,
trailers Content-Length: 17048
Content-Type: multipart/form-data; boundary=-----9yxPJQJxOm5CCaMbP4XHns
```




How FFU's work

- The POST contains the file, but also the answers to the checkboxes on the homepage

Description:

Privacy: Share your file with the world (Recommended)
 For your eyes only (Private) *[Registered users](#) only

Nudity (18+)

I have read and agree to the [TOS](#)

Content-Disposition: form-data; name="descr"

-----9yxPJQJxOm5CCaMbP4XHns

Content-Disposition: form-data; name="is_private"

0

-----9yxPJQJxOm5CCaMbP4XHns

Content-Disposition: form-data; name="TOS"

1

-----9yxPJQJxOm5CCaMbP4XHns

Content-Disposition: form-data; name="pass"



How FFU's work

■ Client-to-Server checks of upload progress

```
GET /uberupload/ubr_get_progress.php?upload_id=6963384d1a981de0b38312900b149ae9 &start_time=1249571828
&total_upload_size=17048 &rnd_id=1249568235728 HTTP/1.1
```

```
User-Agent: Opera/9.22 (Windows NT 5.1; U; en)
Host: dl081.zshare.net:3000
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-bitmap, */*;q=0.1
Accept-Language: en-US,en;q=0.9
Accept-Charset: iso-8859-1, utf-8, utf-16, */q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, */q=0
Referer: http://www.zshare.net/
Cookie: sid=65985202ca9ff4f0fd000e0e4a182d59
      __utma=213908895.1732651668.1249568234.1249568234.1249568234.1
      __utmb=213908895
      __utmc=213908895
      __utmz=213908895.1249568234.1.1.utmccn=(direct)|utmcsr=(direct)|utmcmd=(none)
Cookie2: $Version=1
Connection: Keep-Alive, TE
TE: deflate, gzip, chunked, identity, trailers
```




How FFU's work

■ Server-to-client response after successful upload

Welcome to ^zSHARE

With zSHARE you can upload files, images, videos, audio and flash for free. Simply use the upload form below and start sharing! You can also use zSHARE as your personal file storage: backup your data and protect your files. First Time? Read our [FAQ!](#)

- [Upload now](#)
- [Login](#)
- [Create Free Account](#)
- [Premium](#)
- [FAQ](#)

File Uploaded

The file **khi pics.zip** was successfully uploaded! (4.04MB). You're now ready to share it with unlimited people or keep it as a backup.

Download Link

<http://www.zshare.net/download/637199570b174c9f/>

Link for forums:

[URL = <http://www.zshare.net/download/637199570b174c9f/>]

Direct Link:

<http://www.zshare.net/download/637199570b174c9f/>

Delete Link:

<http://www.zshare.net/delete.html?63719957-7c8893b1k>

[E-mail Me This Info](#)

To receive all the info on the file you uploaded, such as **removal instructions** and **download link**, enter your e-mail address on the field below:

Your e-mail:



Critical piece of collect!

- This one server to client session serves as proof of the success of the upload and it connects the original filename to the URL that will be passed around in E-mail or forum posts

File Uploaded

The file **khi pics.zip** was successfully uploaded! (4.04MB). You're now ready to share it with unlimited people or keep it as a backup.

Download Link

<http://www.zshare.net/download/637199570b174c9f/>

Link for forums:

[URL=http://www.zshare.net/download/637199570b174

Direct Link:

http://www.zshare.net/download/637199570b174c9f/

Delete Link:

http://www.zshare.net/delete.html?63719957-7c8893b1k



How FFU's work

HTTP activity in time order

HTTP Type	Host	URL Path	URL Args
get	www.zshare.net	/	
post	dl081.zshare.net:3000	/cgi-bin/ubr_upload.pl	upload_id=6963384d1a981de0b38312900b149ae9&multiple=0&is_private=0&is_eighteen=0&pass=&descr=
get	dl081.zshare.net:3000	/uberupload/ubr_set_progress.php	upload_id=6963384d1a981de0b38312900b149ae9
get	dl081.zshare.net:3000	/uberupload/ubr_link_upload.php	rnd_id=1249568215088
get	dl081.zshare.net:3000	/index2.php	upload_id=6963384d1a981de0b38312900b149ae9&f_id=tarmim.zip&descr=&multiple=0&pass=&is_private=0&
get	dl081.zshare.net:3000	/uberupload/ubr_get_progress.php	upload_id=6963384d1a981de0b38312900b149ae9&start_time=1249571828&total_upload_size=17048&rnd_id=1
get	dl081.zshare.net:3000	/uberupload/ubr_get_progress.php	upload_id=6963384d1a981de0b38312900b149ae9&start_time=1249571828&total_upload_size=17048&rnd_id=1



How does that activity look in XKS?

Client to server request for the homepage:

GET / HTTP/1.1	
User-Agent:	Opera/9.22 (Windows NT 5.1; U; en)
Host:	www.zshare.net
Accept:	text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language:	en-US,en;q=0.9
Accept-Charset:	iso-8859-1, utf-8, utf-16, *,q=0.1
Accept-Encoding:	deflate, gzip, x-gzip, identity, *,q=0
Cache-Control:	max-age=0
Connection:	close
X-BlueCoat-Via:	0A6F53530F3F63EE

HTTP activity meta-data:

Application Info	Datetime	HTTP T	Host
http://www.zshare.net/	2009-08-06 15:16:13	get	www.zshare.net

Application Type	Application	AppID (+Fingerprints)
filetransfer	filetransfer/web/zshare	filetransfer/web/zshare



How does that activity look in XKS?

Server-to-Client request of the homepage:



HTTP activity meta-data:

Application Info

zSHARE - Free Image, Video, Audio, Flash and File Hosting

HTTP Type

response

Application Type	Application	AppID (+Fingerprints)
filetransfer	filetransfer/web/zshare	filetransfer/web/zshare



How does that activity look in XKS?

Client-to-Server POST of file:

```
POST /cgi-bin/ubr_upload.pl?upload_id=6963384d1a981de0b38312900b149ae9
&multiple=0&is_private=0&is_eighteen=0&pass=&descr=HTTP/1.1
User-Agent: Opera/9.22 (Windows NT 5.1; U; en)
Host: dl081.zshare.net:3000
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg,
image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: en-US,en;q=0.9 Accept-Charset: iso-8859-1, utf-8, utf-16, */*;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, */*;q=0
Expect: 100-continue
Referer: http://www.zshare.net/
Cookie: sid=65985202ca9ff4f0fd000e0e4a182d59
Cookie2: $Version=1 Connection: Keep-Alive, TE TE: deflate, gzip, chunked, identity, trailers
Content-Length: 17048
Content-Type: multipart/form-data; boundary=-----9yxPJQJxOm5CCaMbP4XHns
```

HTTP activity meta-data:

HTTP T	Host	URL Path	URL Args
post	dl081.zshare.net:3000	/cgi-bin/ubr_upload.pl	upload_id=6963384d1a981de0b38312900b149ae9&multiple=0&is_private=0&is_eighteen=0&pass=&descr=

Cookie	Referer	Attachment Filename
sid=65985202ca9ff4f0fd000e0e4a182d59	http://www.zshare.net/	khi pics.zip

Data Length	Session Length	Application Type	Application	AppID (+Fingerprints)
17829	18348	filetransfer	filetransfer/web/zshare/upload	filetransfer/web/zshare/upload compression/pkzip



How does that activity look in XKS?

Client-to-Server checks up upload status:

```
GET /uberupload/ubr_get_progress.php?upload_id=6963384d1a981de0b38312900b149ae9 &start_time=1249571828
&total_upload_size=17078 &mc_id=1249568235728 HTTP/1.1
User-Agent: Opera/9.22 (Windows NT 5.1; U; en)
Host: dl081.zshare.net:3000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/png,image/jpeg,image/gif,image/svg+xml,*/*;q=0.1
Accept-Language: en-US;q=0.9
Accept-Charset: iso-8859-1,utf-8,utf-15,*;q=0.1
Accept-Encoding: deflate,gzip,x-gzip,identity,*;q=0
Referer: http://www.zshare.net/
Cookie: sid=65985202ca9ff4f0fd000e0e4a182d59
      __utma=213908895.1732651568.1249568234.1249568234.1249568234.1
      __utmb=213908895
      __utmc=213908895
      __utmz=213908895.1249568234.1.1.utmcsr=(direct)|utmcs=(direct)|utmcmd=(none)
Cookie2: SVersion=1
Connection: Keep-Alive, TE
TE: deflate,gzip,chunked,identity, trailers
```

HTTP activity meta-data:

HTTP T	Host	URL Path	URL Args
get	dl081.zshare.net:3000	/uberupload/ubr_set_progress.php	upload_id=6963384d1a981de0b38312900b149ae9

Cookie	Referer
sid=65985202ca9ff4f0fd000e0e4a182d59	http://www.zshare.net/

Application	AppID (+Fingerprints)
filetransfer/web/zshare	filetransfer/web/zshare



Introducing the “Web File Transfer” search

- Web File Transfer plug-ins were built to harvest valuable pieces of information which are not pulled out by default in the HTTP activity search
- For example, in the server to client response we see the name of the file that was uploaded, the URL to be used to download the file and the delete key, all great pieces of information!



Web File Transfer search

■ For example:

Welcome to ^zSHARE

With zSHARE you can upload files, images, videos, audio and flash for free. Simply use the upload form below and start sharing! You can also use zSHARE as your personal file storage: backup your data and protect your files. First Time? Read our [FAQ!](#)

- [Upload now](#)
- [Login](#)
- [Create Free Account](#)
- [Premium](#)
- [FAQ](#)

File Uploaded

The file **khi pics.zip** was successfully uploaded! (4.04MB). You're now ready to share it with unlimited people or keep it as a backup.

Download Link

<http://www.zshare.net/download/637199570b174c9f/>

Link for forums:

Direct Link:

Delete Link:

[E-mail Me This Info](#)

To receive all the info on the file you uploaded, such as **removal instructions** and **download link**, enter your e-mail address on the field below:

Your e-mail:



Web File Transfer search

- Web File Transfer plug-ins were built to extract fields like this

File Uploaded

The file **khi pics.zip** was successfully uploaded! (4.04MB). You're now ready to share it with unlimited people or keep it as a backup.

Download Link

<http://www.zshare.net/download/637199570b174c9f/>

Link for forums:

[URL=http://www.zshare.net/download/637199570b174c9f/]

Direct Link:

<http://www.zshare.net/download/637199570b174c9f/>

Delete Link:

<http://www.zshare.net/delete.html?63719957-7c8893b1k>

File URL	Filename
http://www.zshare.net/download/637199570b174c9f/	khi pics.zip

Transfer Type	Upload ID	Delete ID	Site Name
upload	63719957	7c8893b1bf04170771dca3e7f0756a26	zshare.net



Web File Transfer search

Other examples:

File name	File type	File size	Attachments
.html	HTTP/HTML	3072	0

[Expand all](#) | [Collapse all](#)
[Send to Aqility Realtime](#)



PREMIUM-Downloads
PREMIUM Zone

File Movie1_1

Thank you for your upload. Remember to
RapidShare is a file

Your Download-Link #1: <http://rapidshare.com/files/265341718/mpegablePlayer.exe.html>
Your Delete-Link #1: <http://rapidshare.com/files/265341718/mpegablePlayer.exe.html>

**The world's biggest
1-Click Webhoster**

FAQ Imprint
[Fcgrot Premium-password?](#)
WARNING OF PHISHING!

Upload | Download link

1. Download Link

<http://rapidshare.com/files/265341718/mpegablePlayer.exe.html>
MD5: 1B2AAD9F2BBB6A918882127DAFCDD2EB

[Click here to download file](#)

Send download link via e-mail

We send you, and two other recipient of your choice the download and deletion links per e-mail so that you can always access your data.

Name (sender):

(max 64 characters long)

E-mail address of first recipient:

(max 64 characters long)

E-mail address of additional recipient:

(max 64 characters long)

E-mail address of additional recipient:

(max 64 characters long)

Short message to the recipient:

(max 1000 characters long)

[Information](#)

[About us](#) | [Terms of use](#) | [Imprint](#)



Searching on FFU's in XKS

- When you see an FFU URL passed around, you can use the HTTP activity parser to see if anyone went to that URL.
- Use the HTTP activity search and simply copy and paste the URL into the "URL field builder"
- Make sure to add a valid foreign IP address or foreign country code to your search to make it USSID18 compliant!!



Searching on FFU's in XKS

- For example, if we see this URL passed around in traffic: `http://www.zshare.net/download/6365962739d34eba`

Search: HTTP Activity

Query Name:

Justification:

FFU URL used by CT target

[Recent Justifications](#)

Additional Justification:

Miranda Number:

Datetime:

1 Month

Start:

2009-07-12

00

URL Field Builder

Enter a URL that will be automatically parsed to populate the host, path, and argument fields:

`http://www.zshare.net/download/6365962739d34eba`

Enter

Cancel

HTTP Type:

Host:

[Populate with URL Field Builder]

URL Path:



Searching on FFU's in XKS

- **Make sure to and your search with a valid foreign target, like IP address or country or city code!!**

HTTP Type:

Host: [\[Populate with URL Field Builder\]](#)

URL Path:

IP Address: [\[IP Address Field Builder\]](#)

IP Address: [\[IP Address Field Builder\]](#)

Port:

Port:

Country:

Country:



Searching on FFU's in XKS

- It's also worth it to search the URL as the "referrer" and again remember to add something "foreign"

Referer:

IP Address: From  [\[IP Address Field Builder\]](#)

IP Address: To  [\[IP Address Field Builder\]](#)

Port: From

Port: To

Country: From

Country: To



Searching on FFU's in XKS

- To find all files being uploaded to FFU's from a given IP address/range or city/country code use the HTTP activity query

HTTP Type: ▼

Attachment Filename:

Application: ▼

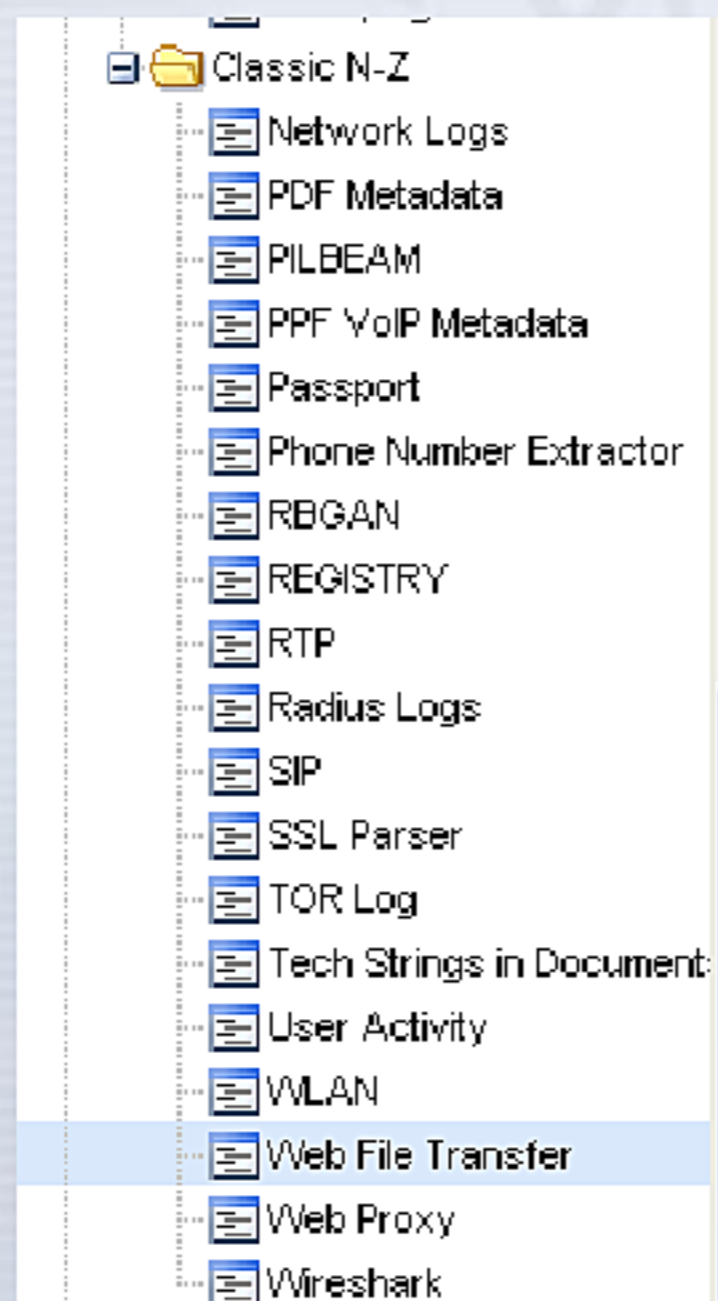
Country: ▼ From ▼

IP Address: From ▼



Searching on FFU's in XKS

- If you want to try to find who uploaded the file that generated that URL, use the Web File Transfer Plug-in





Searching on FFU's in XKS

- To find all file upload success web-pages, which have the filename and the FFU URL, use the Web File Transfer Search

Transfer Type:

Site Name:

IP Address: To

Country: To



Searching on FFU's in XKS

- To try to find the filename associated with a URL, enter in the URL into the "File URL" field, again remember to add something "foreign"

Fields - Advanced Features - Show Hidden Search Fields - Clear Search Values - Reload Last Search Values

Search: Web File Transfer

Query Name:

Justification: [Reset Justifications](#)

Additional Justification:

Miranda Number:

Datetime: Start: Stop:

File URL:

Filename:

File Type:

Description:

File Size:

IP Address: From [\[IP Address Field Builder\]](#)

IP Address: To [\[IP Address Field Builder\]](#)

Port: From

Port: To

Country: From

Country: To

City (IP): From