Reconstructing Streamed Video Content: A Case Study on YouTube and Facebook Live Stream Content in the Chrome Web Browser Cache

Dr Graeme Horsman - g.horsman@tees.ac.uk

Teesside University, United Kingdom.

First….apologies that I could not be there in person…

….but thanks for being allowed to contribute….

Context

Video streaming has been reported as being involved in the following offences:-

- **Copyright infringement and piracy** - (BBC News, 2017f; BBC News, 2017j)
- **Assaults** - (Brunty, 2016)
- **Trolling and harassment** - (BBC News, 2017h)
- **Vehicle accidents** - (BBC News, 2015; BBC News, 2017a).
- **Robbery** - (Irwin-Rogers and Pinkney, 2017).
- **Live streaming of child abuse** - (BBC News, 2016; BBC News, 2017b; BBC News, 2017c; BBC News, 2017d; BBC News, 2017e; BBC News, 2017g; BBC News, 2017i; BBC News, 2017l; Yuhas, 2017)
    - **Facebook's 'live' function** have both been singled out for their use in a number of recent child abuse incidents (BBC News; 2016a; BBC News, 2017c; Chuck, 2016; nbc4i.com, 2016; Ng, 2016; Solon, 2017).

Regulatory Challenges

- The use of live-streaming in cases of child sexual abuse is expected to increase as the technology develops and underlying broadband infrastructures allow for its use (Europol, 2015).

- Capturing of streamed content and re-distribution.

- Identifying what involvement a suspect has had in terms of engaging with a stream.
  - What did they watch?
  - How much did they watch?
  - Did they engage with the stream - For example Periscope's chat whilst broadcasting function.

Legislation

- Section 176 of the Policing and Crime Act 2017:- The inclusion of streaming as a form of ‘sexual exploitation’.

- Traditional offences under the Protection of Children Act 1978 and Criminal Justice Act 1988.
    - Making
    - Possession

Set-up

Things to note:-

1. Tests were run using Chrome.
    a. Expect the same results in both.

1. Tests ran live.
    a. Cache captured using ChromeCacheView.
    b. On the fly parsing.

1. Potential time sensitivity.
    a. At the time of testing (Dec - April), this works.
    b. Subject to changes in stream protocols and the way browsers handles this action

1. None of this is available if the user streams using a browser’s private mode.

FACEBOOK Live

Issues

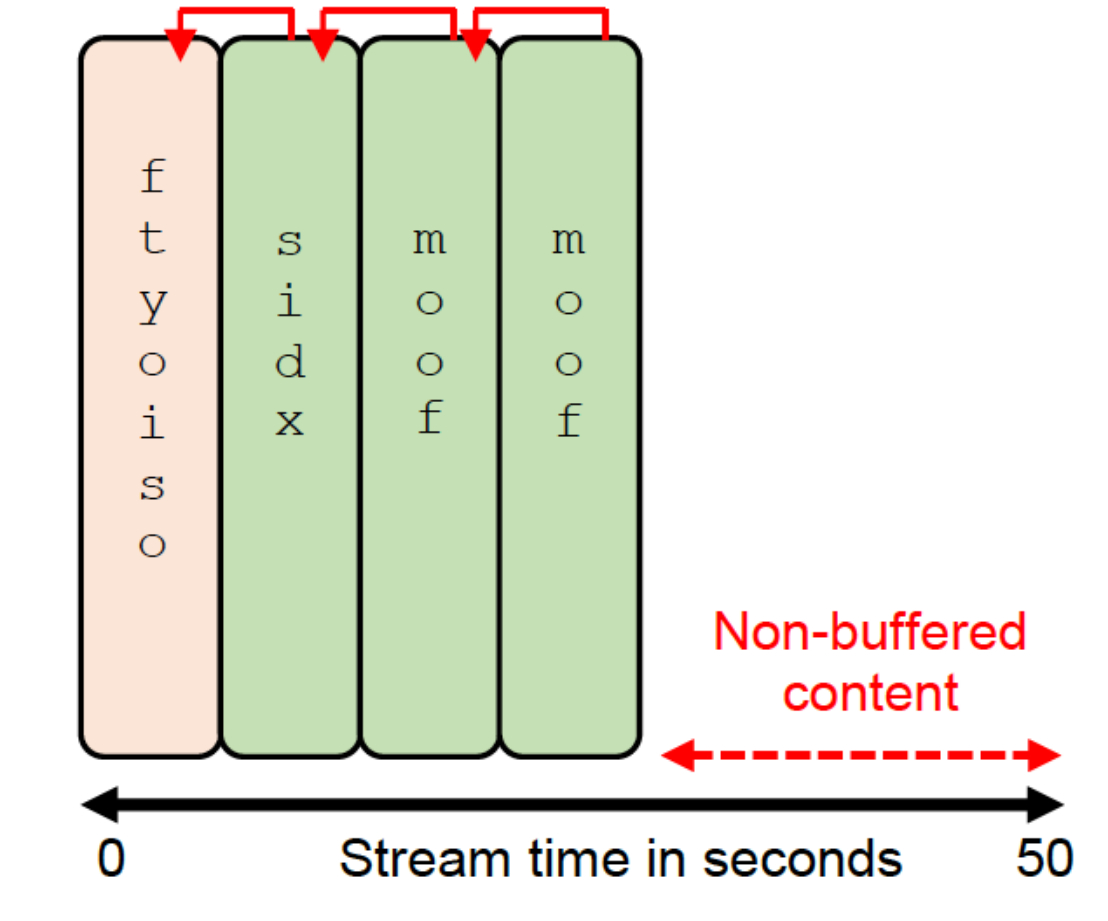
1. Testing involved Facebook Live in the Chrome browser, **NOT** the app.
    a. Later work.

1. Facebook Live videos are not cached.
    a. Nightmare.....but, once finished, they may be hosted....and if this content is viewed it is cached!

1. ONLY buffered content is cached.
    a. The benefit / downside to this is that you can tell what part of a stream was accessible to an individual based on the cache.
    b. Cached content does **NOT** mean viewed content
        i. For example, Youtube buffers in about 30 second chunks.

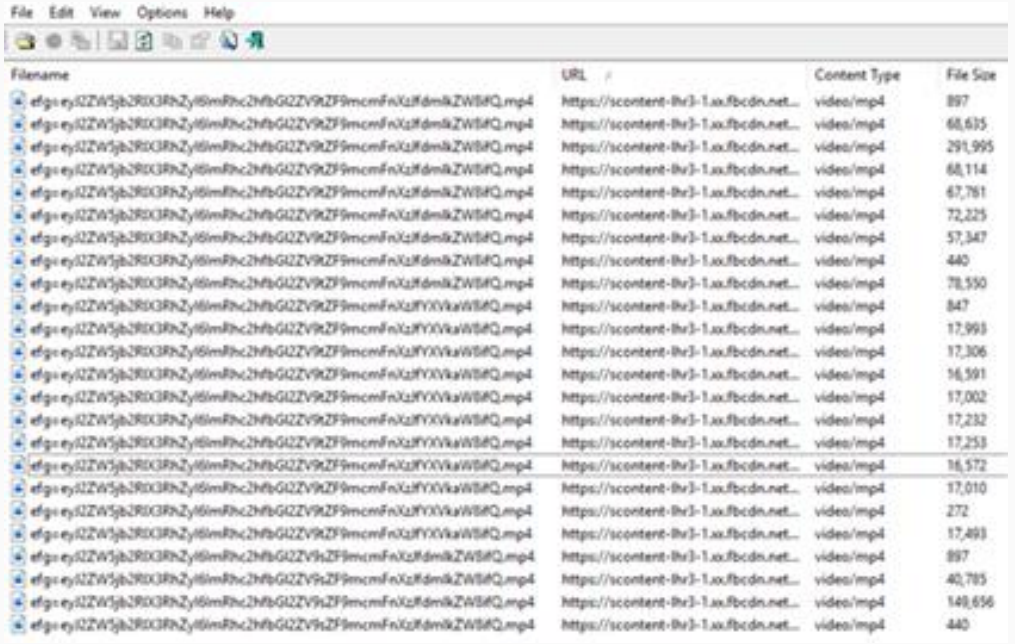
Structure

Typically, stream rebuild fragments will appear as noted in Figure 7, with a typical .mp4 structured header (`ftyoiso` identifier), followed by a `sidx` identifier fragment and finally a series of `moof` identifier fragments. Only buffered content of a Facebook Live replayed video can be recovered.



So what does the cache look like?

- .mp4 files pushed into the cache.
- All varying sizes.
- **NONE** are playable as individual files.

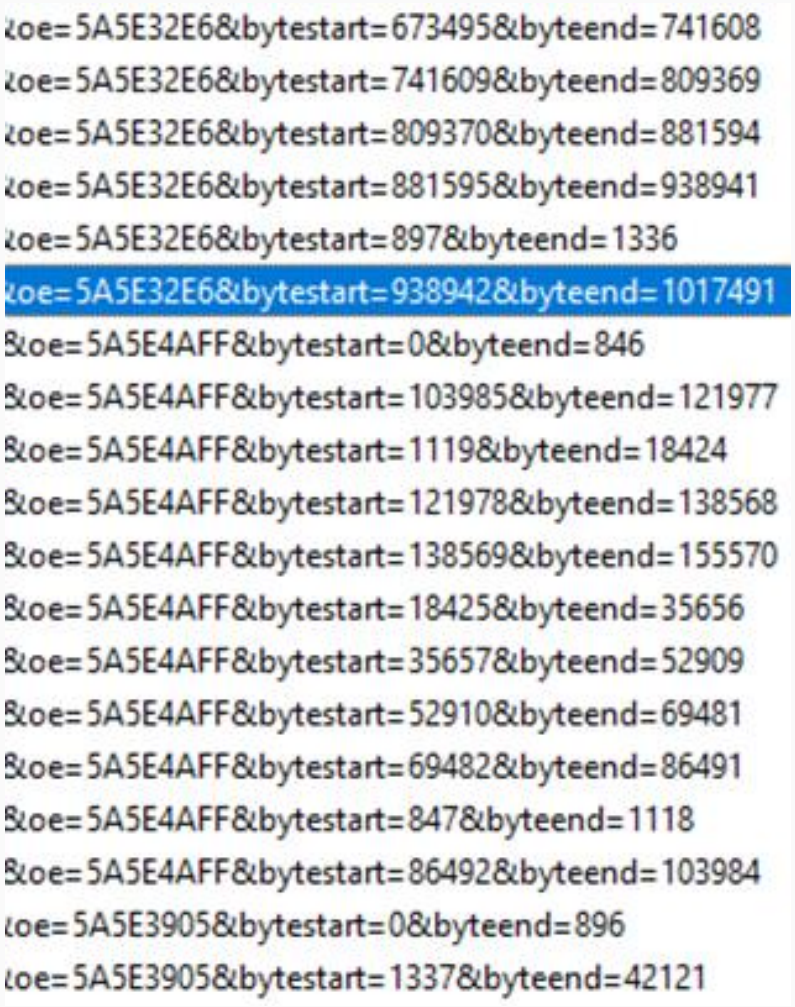


TYPICAL STRUCTURE:-

https://scontent-lhr3-1.xx.fbcdn.net/v/t42.1790-29/26947798_1548879368500753_3538282435986849792_n.mp4?efg=eyJ2ZW5jb2RlX3RhZyI6ImRhc2hfbGl2ZV9tZF9mcmFnXzJfYXVkaW8ifQ%3D%3D&oh=a5c44f0172736933195c1eaf2e35bb9d&**oe=5A5E4AFF**&**byteend=**69481

Rebuild

To rebuild the stream, the `oe=`, `bytestart=` and `byteend=` attributes are important. Testing indicates that the `oe=` attribute acts as a stream identifier. Here we provide an example where despite only one stream being viewed, cached stream fragments are sorted by their `oe=` attribute, where only matching `oe=` values form part of the same stream rebuild. The `bytestart=` and `byteend=` attributes denote the order of concatenation.



Points to Note

1. Stream reassembly must occur with the correct `oe=` values and in byte order. In reference back to previous figure, 3 streams are present, one is the video. No way to tell, must rebuild all.

1. If you run mass media carving/recovery/file identification processes for video in typical forensic tools you may not get anything back.

1. VLC will not play these files as individual entities.

1. If you want them to play, you have to concatenate them **IN ORDER**.

1. `bytestart=` and `byteend=` attributes must be used in incremental order to determine the order of concatenation, they are not always perfectly numerically aligned (for example, not always 1, 2, 3, 4 – sometimes 1, 3, 4, 6). Providing they were in incremental numerical value order, testing indicated that a stream rebuild could still be achieved.

YouTube

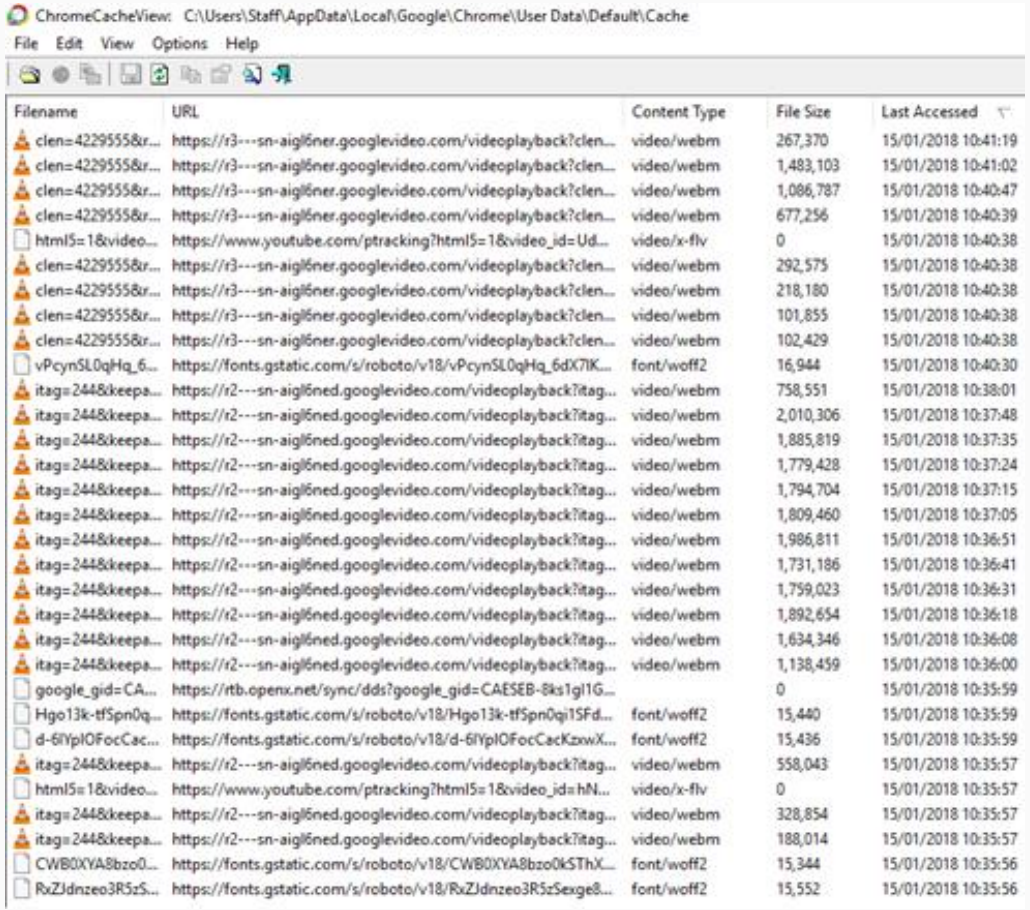
YouTube

- YouTube (www.youtube.com) is a video sharing and streaming platform owned by Google and maintains significant popularity with a reported estimate of 184 million users in the U.S. alone (Statista, 2018).
- A reported 400 hours of video uploaded every minute (Schindler, 2017).
- Mechanisms for child protection and their apparent failures have been highlighted (BBC News, 2017b) with reports of up to 100,000 predatory accounts leaving indecent comments on video material (BBC News, 2017c).
- Reports of indecent content and videos depicting child characters in inappropriate situations (designed to trick child viewers into watching) have been noted (BBC News, 2017d; 2018b).
- In November 2017, YouTube were reported to have removed almost 50,000 videos documenting extremist content,

An example

1. Test stream creates 41 .webm files.

2. Only the first 2 seconds of the stream is viewable. The rest will not play in VLC or other tools.



Filename	URL	Content Type	File Size	Last Accessed
clen=4229555&r...	https://r3---sn-aigl6ner.googlevideo.com/videoplayback?clen...	video/webm	267,370	15/01/2018 10:41:19
clen=4229555&r...	https://r3---sn-aigl6ner.googlevideo.com/videoplayback?clen...	video/webm	1,483,103	15/01/2018 10:41:02
clen=4229555&r...	https://r3---sn-aigl6ner.googlevideo.com/videoplayback?clen...	video/webm	1,086,787	15/01/2018 10:40:47
clen=4229555&r...	https://r3---sn-aigl6ner.googlevideo.com/videoplayback?clen...	video/webm	677,256	15/01/2018 10:40:39
html5=1&video...	https://www.youtube.com/ptracking?html5=1&video_id=Ud...	video/x-flv	0	15/01/2018 10:40:38
clen=4229555&r...	https://r3---sn-aigl6ner.googlevideo.com/videoplayback?clen...	video/webm	292,575	15/01/2018 10:40:38
clen=4229555&r...	https://r3---sn-aigl6ner.googlevideo.com/videoplayback?clen...	video/webm	218,180	15/01/2018 10:40:38
clen=4229555&r...	https://r3---sn-aigl6ner.googlevideo.com/videoplayback?clen...	video/webm	101,855	15/01/2018 10:40:38
clen=4229555&r...	https://r3---sn-aigl6ner.googlevideo.com/videoplayback?clen...	video/webm	102,429	15/01/2018 10:40:38
vPcynSL0qHq_6...	https://fonts.gstatic.com/s/roboto/v18/vPcynSL0qHq_6dX7lK...	font/woff2	16,944	15/01/2018 10:40:30
itag=244&keepa...	https://r2---sn-aigl6ned.googlevideo.com/videoplayback?itag...	video/webm	758,551	15/01/2018 10:38:01
itag=244&keepa...	https://r2---sn-aigl6ned.googlevideo.com/videoplayback?itag...	video/webm	2,010,306	15/01/2018 10:37:48
itag=244&keepa...	https://r2---sn-aigl6ned.googlevideo.com/videoplayback?itag...	video/webm	1,885,819	15/01/2018 10:37:35
itag=244&keepa...	https://r2---sn-aigl6ned.googlevideo.com/videoplayback?itag...	video/webm	1,779,428	15/01/2018 10:37:24
itag=244&keepa...	https://r2---sn-aigl6ned.googlevideo.com/videoplayback?itag...	video/webm	1,794,704	15/01/2018 10:37:15
itag=244&keepa...	https://r2---sn-aigl6ned.googlevideo.com/videoplayback?itag...	video/webm	1,809,460	15/01/2018 10:37:05
itag=244&keepa...	https://r2---sn-aigl6ned.googlevideo.com/videoplayback?itag...	video/webm	1,986,811	15/01/2018 10:36:51
itag=244&keepa...	https://r2---sn-aigl6ned.googlevideo.com/videoplayback?itag...	video/webm	1,731,186	15/01/2018 10:36:41
itag=244&keepa...	https://r2---sn-aigl6ned.googlevideo.com/videoplayback?itag...	video/webm	1,759,023	15/01/2018 10:36:31
itag=244&keepa...	https://r2---sn-aigl6ned.googlevideo.com/videoplayback?itag...	video/webm	1,892,654	15/01/2018 10:36:18
itag=244&keepa...	https://r2---sn-aigl6ned.googlevideo.com/videoplayback?itag...	video/webm	1,634,346	15/01/2018 10:36:08
itag=244&keepa...	https://r2---sn-aigl6ned.googlevideo.com/videoplayback?itag...	video/webm	1,138,459	15/01/2018 10:36:00
google_gid=CA...	https://rtb.openx.net/sync/dds?google_gid=CAESEB-8ks1gl1G...		0	15/01/2018 10:35:59
Hgo13k-tfSpn0q...	https://fonts.gstatic.com/s/roboto/v18/Hgo13k-tfSpn0qi1SFd...	font/woff2	15,440	15/01/2018 10:35:59
d-6IYplOFocCac...	https://fonts.gstatic.com/s/roboto/v18/d-6IYplOFocCacKzxwX...	font/woff2	15,436	15/01/2018 10:35:59
itag=244&keepa...	https://r2---sn-aigl6ned.googlevideo.com/videoplayback?itag...	video/webm	558,043	15/01/2018 10:35:57
html5=1&video...	https://www.youtube.com/ptracking?html5=1&video_id=hN...	video/x-flv	0	15/01/2018 10:35:57
itag=244&keepa...	https://r2---sn-aigl6ned.googlevideo.com/videoplayback?itag...	video/webm	328,854	15/01/2018 10:35:57
itag=244&keepa...	https://r2---sn-aigl6ned.googlevideo.com/videoplayback?itag...	video/webm	188,014	15/01/2018 10:35:57
CWB0XYA8bzo0...	https://fonts.gstatic.com/s/roboto/v18/CWB0XYA8bzo0kSThX...	font/woff2	15,344	15/01/2018 10:35:56
RxZJdnzeo3R5zS...	https://fonts.gstatic.com/s/roboto/v18/RxZJdnzeo3R5zSexge8...	font/woff2	15,552	15/01/2018 10:35:56

Reconstruction

Fragment order and concatenation is key if you want to see this stream...

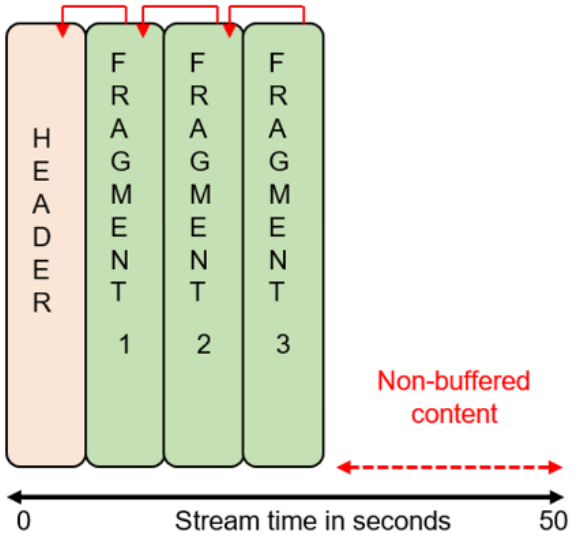
https://r2---sn-aigl6ned.googlevideo.com/videoplayback?itag=244&keepalive=yes&lmt=1515578817467917&key=yt6&signature=76C58D7F78D783433894A5035F5782BC42B24479.1267C0A3034DC4EBDA3C7968798118B3810E0BE3&ms=au&mv=m&mt=1516012566&requiressl=yes&ip=152.105.118.127&ipbits=0&gcr=gb&pl=16&id=o-AE1mirNM9fvhqmgotXSh29VDXx1bmxZr2dzVu_HMWonX&**mime=video%2Fwebm**&mn=sn-aigl6ned&mm=31&expire=1516034260&ei=dIRcWoSZI4LgV-T7ucAH&initcwndbps=1595000&gir=yes&**dur=272.440**&source=youtube&clen=21255658&sparams=aitags%2Cclen%2Cdur%2Cei%2Cgcr%2Cgir%2Cid%2Cinitcwndbps%2Cip%2Cipbits%2Citag%2Ckeepalive%2Clmt%2Cmime%2Cmm%2Cmn%2Cms%2Cmv%2Cpl%2Crequiressl%2Csource%2Cexpire&aitags=133%2C134%2C135%2C136%2C137%2C160%2C242%2C243%2C244%2C247%2C248%2C278&ratebypass=yes&alr=yes&cpn=QhnO2WvdKbz3nFlQ&c=WEB&cver=2.20180111&**range=0-188013**&rn=0&rbuf=0

Reconstruction

- The order must be correct otherwise the video won't play.
- Fragments don't have a defined signature. **EMPHASIS SHOULD BE PLACED ON EXAMINING THE CACHE.**
- **ONLY BUFFERED CONTENT IS IN THE CACHE.**

Table 1: A breakdown of a hypothetical reconstruction of a YouTube stream

File Order	File Order	Range (example values)	File Signature
Header	1	0-188013	0x1A 0x45 0xDF 0xA3 0x9F 0x42 0x86 0x81 0x01 0x42 0xF7 0x81 0x01 0x42 0xF2 0x81 0x04 0x42 0xF3 0x81 0x08 0x42 0x82 0x84 0x77 0x65 0x62 0x6D 0x42
Data Fragment	2	188014-35644	N/A
Data Fragment	3	35645-611485	N/A
Data Fragment	4	611486-983432	N/A



Conclusions

- Stream content can be rebuilt.
- Mass media recovery processes may not collect and display this - be careful not to miss it because it is there.
- Concatenation of fragments is required in order to build the video.
- Make sure fragments are in the correct order.

Future Work

- In-depth study has been completed on Periscope.
- Expand analysis to range of services.
- Move to the mobile platform.