Digital Investigation 26 (2018) S30–S37

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

DFRWS 2018 USA — Proceedings of the Eighteenth Annual DFRWS USA

Reconstructing streamed video content: A case study on YouTube and Facebook Live stream content in the Chrome web browser cache

Graeme Horsman

School of Science, Engineering and Design, University of Teesside, Campus Heart, Southfield Rd, Middlesbrough, TS1 3BX, United Kingdom

Keywords:
Digital forensics
Video stream
Video forensics
YouTube
Facebook Live

ABSTRACT

With the increased popularity of online video streaming comes the risk of this technology's subsequent abuse. With a number of cases noted in 2017 where individuals have engaged with illegal or policy breaching video content, digital forensics practitioners are often tasked with investigating the subsequent 'fingerprint' of such acts. This is often to determine both the content of a stream in question, and, how it has been interacted with, typically from an analysis of data residing on a suspect's local device. This article provides an examination of the forensic procedures required to identify and reconstruct cached video stream data using both YouTube and Facebook Live as example case studies. Stream reconstruction methodologies are offered where results show that where a YouTube and Facebook Live video have been played, buffered video stream data can be reassembled to produce a viewable video clip of content.

1. Introduction

To highlight the issues surrounding on-line video streaming, initial reference is drawn to the following comments made by the National Crime Agency in December 2017.

> *"The use of live streaming platforms by online sex offenders is increasing … During a recent week of intensification to tackle child sexual exploitation and abuse, police and NCA operations across the UK safeguarded 245 children and arrested 192 people, 18 of whom were in a position of trust. 30% of those cases involved some of the highest harm offences including live streaming, blackmail and grooming … Intelligence from the NCA and police forces shows that that dangerous offenders are capitalising on the immediacy of contact that live streaming offers"* (National Crime Agency, 2017a).

Online video streaming platforms now provide users with an opportunity to share content and to observe (via streaming) video material posted by others, without exhibiting ownership of it in terms of intentionally downloading and storing video content. A significant proportion of Internet users now watch video content online (Statista, 2018b) where 'as of 2017, 81.2% of online users in the U.S. alone (over 200 million) accessed digital video content' (Statista, 2018c, 2018d), a figure which is predicted to rise. With such volumes of traffic come regulatory problems linked to both the uploading and distribution of video content in breach of law and platform policies, and, the subsequent viewing and engagement with such material. Whilst mainstream vendors may have the resources to tackle such issues, smaller services may not, creating a challenge for law enforcement when attempting to effectively respond to an incident of this type. Whilst the discovery of an illegal/policy breaching video online may lead to consequences for the video 'owner' or a hosting/streaming service provider, identifying who has viewed and interacted with the video may lead to further liability for such individuals. This is apparent in cases of streamed indecent content where the (National Crime Agency (2017b; 2017c; 2017d; 2017e)) in 2017 have noted numerous instances of users prosecuted for indecent imagery offences under English law after interacting with online indecent video material. Extremist video content has also attracted regulatory interest and response, with the United Kingdom Home Secretary Amber Rudd seeking to impose stronger penalties on those who repeatedly view terrorist material online in an attempt to strengthen existing regulation under areas such as section 58 of the Terrorism Act 2000 (Travis, 2017).

Acts of video streaming (whether live or the replay of prerecorded hosted content) can be associated with a number of potential offences and where a suspect's device has been seized,

E-mail address: g.horsman@tees.ac.uk.

https://doi.org/10.1016/j.diin.2018.04.017
1742-2876/

forensic analysis may be required to identify any potential streamed content. Whilst Internet history records may in some instances provide a pointer to a hosted video that has been accessed, this may not always be an effective at identifying any streamed content. Where a video has since been removed by a provider (no longer accessible online by a practitioner for verification of content), locally cached stream data (providing it can be interpreted) may be the only source of information remaining to identify a streams content and context. Further in offences involving indecent imagery, the identification and recovery of imagery left behind by a stream on a local device may facilitate a charge of possession or making indecent imagery under English law (see Protection of Children Act 1978 and Criminal Justice Act 1988).

With regards a forensic examination of the impact and recovery of streamed video on a local device, limited information exists. This article provides one of the first commentaries in this area, and aims to support those carrying out investigations of this type to ensure effective evidence recovery and interpretation. In doing so, this work addresses the following questions.

1. Is streamed video content stored on a local device when viewed? And if so;
   a) Can streamed video content be recovered and viewed?
   b) Is it possible to determine how much of a video has been viewed?

Within the confines of this article two case studies are presented, an examination of YouTube and Facebook Live video streams. Due to limitations with article size, only the Chrome Internet browser has been examined as a platform for accessing and streaming video content. Both testing methodologies and results are offered.

2. YouTube

YouTube (www.youtube.com) is a video sharing and streaming service owned by Google and maintains significant popularity with a reported estimate of 184 million users in the U.S. alone (Statista, 2018), with a reported 400 h of video uploaded every minute (Schindler, 2017). Whilst the platform offers a popular source of material across a number of topic areas, it has also attracted criticism, particularly focused at its regulation of resident content. 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). Further, 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; 2017e; 2018b). In November 2017, YouTube were reported to have removed almost 50,000 videos documenting extremist content, however, were criticized for an apparent slowness to act (BBC News, 2017a). In addition, concerns have also been raised due to the hosting of videos depicting anti-Semitic and gang culture (BBC News, 2017f, 2018a).

Where the investigation of a suspect leads to the analysis of their YouTube viewing habits, resident Internet history may provide some support. A standard YouTube URL is structured as follows: https://www.youtube.com/watch?v=mXFjwihUO00 where there URL itself is prefixed with a unique identifier (bolded above) for the YouTube video itself. In some cases, a practitioner can search for the video using this identifier and verify its content. However, this process alone may not address the following two points of concern.

1. Video removal: A user may view a video that has since been removed before a practitioner inspection can take place. In this case, a practitioner may identify a suspected URL, but be unable to locate the video on the YouTube site. Whilst it may be possible to request an account disclosure from YouTube, a record of such information may no longer exist, or limited organizational resources may deem disclosure routes impractical.
2. Behavior: Where a video is of large length, determining how much of a video a user has watched and what particular content may be of evidential value and could provide.

In the cases noted above, resident cached video data may provide the only source of determining the context of a streamed video. As a result, the remainder of Section 2 offers an examination of the impact of YouTube streams in the Chrome web browser cache.

2.1. Preliminary approach

To provide an initial insight into the challenges of investigating stream caching, an initial test designed to explore the use of file identification, parsing and recovery processes to examine the browser cache following the viewing of a test stream was ran. This was intended to simulate traditional analysis approaches, which involve large-scale file recovery and viewing processes typically undertaken through the running of automated procedural scripts. The following methodology has been implemented.

2.1.1. Preparation

To start, a standard clean install of the Windows 10 operating system was implemented and the Chrome (version 63.0.3239.132 (latest at time of testing)) browser was installed (and unused).

2.1.2. Test data

A uniquely identifiable YouTube video was chosen as suitable test data and its content recorded. This would allow for a visual identification and verification of any subsequently recovered streamed content (following the analysis stage) on the local machine resulting from the test stream. The chrome cache folders (`C:\Users\Staff\AppData\Local\Google\Chrome\User Data\Default\Cache`) were verified as empty to prevent contamination by any existing data.

2.1.3. Viewing the stream

The test YouTube video's URL was entered into the Chrome browser window and the video was played in full. The browser was then closed and the machine was shut down and imaged.

2.1.4. Analysis

X-Ways forensics version 19.3's comprehensive search options were utilized to recover (identify or carve, and reconstruct) all potential image, video and internet related data. Reliance was placed on automated media gathering processes to simulate traditional case procedures that are often used in forensic investigations to pre-process any existing media files *en-masse* for later review. On completion, four still thumbnail-sized cached images (`.jpg`) denoting content (video frames) contained within the stream were recovered by both tools (located at `C:\Users\Staff\AppData\Local\Google\Chrome\User Data\Default\Cache`). 41 `.webm` (a compressed video stream format (FileInfo, n.d.)) files were also located following the parsing of the Chrome cache metadata and cache data files. All `.webm` were exported given they are reported to be video stream files and opened using VLC media player version 2.2.6 where only one file was playable, containing content from the first 3 s of the test video stream. All other `.webm` files returned errors upon attempting to play.