# Cloud Investigations of Illegal IPTV Networks

John Sheppard
*Emerging Devices Lab*
*Department of Computing and Mathematics, School of Science*
*Waterford Institute of Technology*
*Waterford, Ireland*
*Email: jsheppard@wit.ie*

*Abstract*—**Kodi software has gained much attention in recent years due to its powerful capabilities for streaming legal and illegal media sources. This has led to numerous court cases and media reports around piracy and copyright infringement. This paper examines some of the most popular Kodi video addons on a Raspberry Pi 3 running Open Source Media Center (OSMC). There are a variety of different roles involved in the Kodi community such as normal users, addon authors and distributors. This paper identifies and defines these key roles. It looks at the relationships between addons and their authors and distributors. It shows how cloud evidence can be used to connect devices to the addon distributors. It further investigates the networks found among these authors and distributors using GraphQL in the GitHub cloud.**

Cloud Forensics, Cloud Investigations, Cloud Evidence, GitHub, Streaming, Kodi, Addons, GraphQL, Piracy

## 1. Introduction

IPTV services have been growing in popularity in recent years. Some of these cloud services are offered by TV networks as free video on demand type catch up services, others are offered through licensed monthly subscription fees. A further category is illegally pirated streaming services which can be found and utilised through a combination of cheap and easily obtainable hardware, and open source software.

IPTV is a subset of Over-The-Top (OTT) services. An over-the-top (OTT) service is an online service that can be regarded as potentially substituting for traditional telecommunications and audiovisual services such as voice telephony, SMS and television. An online service is defined as a service that utilises the public internet for delivery in contrast to a managed service, which has control over access to its network [2]. Legal OTT IPTV services can be further categorised by their revenue model as subscription-based (SVOD), advertising-based (AVOD), transactional-based (TVOD) and premium-based (PVOD). SVOD offer monthly packages such as Netflix or NowTV. AVOD services stream free content to the user but show advertisements either before, during or after the content. These services include Crackle and Youtube. TVOD users can purchase a one off subscription to rent content for an amount of time, similar to pay per view, or to download and own content permanently. An example of such a service is offered by iTunes. PVOD is slightly newer than the others and is being offered by movie studios to allow users to access new movies very shortly after their theatre release and earlier than TVOD at a higher fee.

IPTV streaming services have been in the spotlight for the streaming of pirated content. There have been many high profile court cases taken by the TV and movie industries to protect their content. ISP's have been asked in the courts to help fight streaming piracy by filtering connections and blocking traffic to these streaming providers. In late 2017 the Motion Pictures Association of America claimed that there are 38 million Kodi users worldwide. Of these 26 million are pirating illlegal content [3]. Xbox Media Center (XBMC) Foundation, who develop Kodi, could not comment on these figure "because we don't watch what our users are doing, we have no way of knowing how many do what with regards to streaming" [4]. TVaddons, a major addon repository, did claim to have 39 million active users per month when it was taken offline. TVaddons has since returned and as of January 2018 has 19 million active monthly users [5].

Authors of the addons that enable this activity have been issued cease and desist letters. In 2017 one of the largest illegal IPTV distribution networks was dismantled. The crime gang behind it owned two European ISPs. One was based in Spain and the other in Bulgaria [6].

## 2. Related Work

These systems operate in cloud environments. The addon repositories are stored in, installed from and updated through the cloud. On the piracy side content is streamed from cloud servers to local devices. Commonly there are three areas considered for analysis in a cloud investigation, data at rest on the client side, data in transit and data at rest on the server side [1]. While there has been numerous studies examining interactions between Android devices and the cloud, these tend to focus on smartphones and tablets, and on the artefacts left behind on these devices after communications with cloud storage services [7] and [8]. There have also been studies that have looked at individual televisions such as LG [10] and Samsung [11]. These studies tend to focus on data acquisition issues and on the artefacts left on the devices. The importance of the interaction between IoT devices and cloud computing back-ends is highlighted in [12] and [13].

Cloud services can provide valuable insight into a digital forensic investigation. Several authors have analysed the GitHub cloud. The GHTorrent project used the GitHub REST API V3 to collect data from GitHub and has made their tools and datasets available [15]. Data has also been collected from the GitHub cloud service and mined for association rules in order to determine the success of open source software projects. Based on the success of a project being considered to be over 1000 downloads they identified key features that could be associated with success [9].

## 3. Architeture

IPTV networks consist of a streaming device, that is connected to a screen, and that has access to the internet. These devices run an operating system with streaming software installed. This streaming software is configured to talk to cloud services to obtain IPTV data or for the maintenance and updating of the device.

Kodi is an open source media centre developed by non-profit technology consortium XBMC. It can reside on multiple common operating systems and is compatible with many devices. It is used for streaming music and video from a users private library on their own network or from public sources over the internet. It is highly customisable through the use of applications known as addons. These addons allow Kodi user's to stream content to a Kodi device. Addons, written by third party developers, are easily installed through the Kodi interface by specifying a repository or ”repo” url to connect to. This architecture can be seen in Figure 1 [14].

## 4. Kodi Devices

IPTV services can be streamed to a variety of hardware devices such as smart TVs, PCs, Macs, tablets, phones and specialised devices. These specialised devices include Amazon Fire Stick, Roku TV streaming stick, Android TV Boxes, Apple TV, OSMC's Vero 4K and custom Raspberry Pi's. Other devices such as Google Chromecast allow the casting of streamed content from one device to be mirrored to a larger screen. Streaming devices offer a range of different VOD software solutions. With the exception of the Apple TV, these specialist hardware devices tend to be either Linux-based or Android-based. Linux-based example are the Roku TV Streaming Stick, OSMC's Vero 4k and Raspberry Pi solutions. Popular Android systems include the Amazon Fire TV Stick, the MXQ Pro and the Nvidia Shield streaming boxes.

Netflix, Youtube and Kodi are among the most common VOD applications in use. Netflix offers SVOD and Youtube offers AVOD. Kodi allows users to stream from their own private media libraries or to stream VOD via 'addons'. Kodi exists in three different flavours. Open Source Media Center (OSMC), Libre Embedded Linux Entertainment Center (LibreELEC) and Open Embedded Linux Entertainment Center (OpenELEC). Of these three, OSMC is the most advanced system allowing for the installation of Linux applications through the OSMC App store. The increase in hardware power associated with Kodi devices is leading to a larger user adoption of OSMC. In February 2016 NIST published CVE-2016-2230 with a critical CVSS severity score of 9.8 relating to a hardcoded root password [16]. In June 2017 NIST further published CVE-2017-6445 as the auto update feature of OpenELEC did not use encrypted connections or signed updates leaving it vulnerable to a man in the middle attack [17].

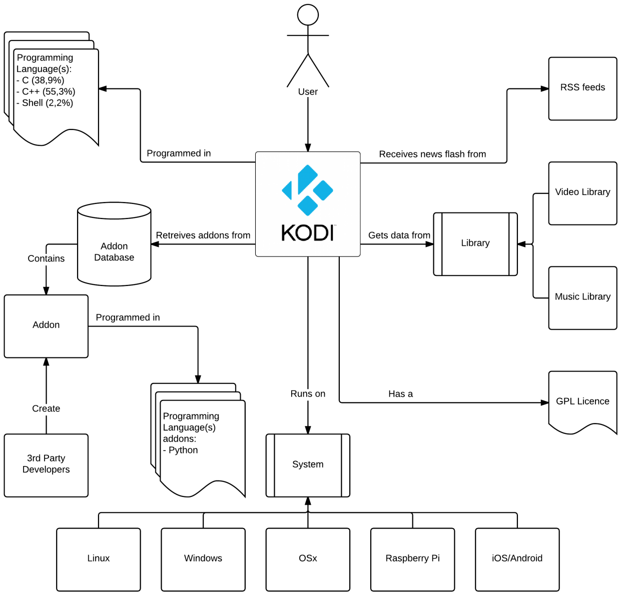


Figure 1. Kodi Architecture.

### 4.1. Local Data Acquisition

Investigation of these devices has shown varying levels of access to the underlying data. Android boxes allow some access to the user's data by enabling USB debugging mode. The devices can then be accessed through the Android Debug Bridge (ADB). Root access is possible depending on the Android device in use. Some older Fire TV sticks allow software rooting while others require the device to be disassembled and some desoldering in order to access the eMMC chip. Other Android boxes may be rooted dependent on available firmware for particular boxes.

Data acquisition of linux-based systems has varying levels of complexity. When running OSMC on a Raspberry Pi 3 or Vero 4k box, access to the devices can be obtained via SSH. The Roku TV Streaming Stick first needs to be entered into developer mode. It contains two network IP addresses which allows telnet access to port 8085 [18]. This is currently being investigated.

The device investigated for this paper is a Raspberry Pi 3 running OSMC. The SD card used was first sanitised and then formatted as FAT. An OSMC image for Rapsberry Pi, OSMC_TGT_rbp2_20180316, was installed through OSMC's qt_host_installer application using a Mac Book Pro. The Pi was configured for a wired network and debugging was enabled on the device.

An online review of the most popular Kodi video addons as of March 2018 was conducted and based on this eight of the most popular addons were installed to the device. [21] [22] [23] [24] [25]. With these addons, users are capable of streaming illegal pirated content such as movies and TV show in 720p, 1080p, and UHD 4K resolution from cyberlockers. These addons account for the most popular 92% of Kodi addons [21] and can be seen in Table 1.

TABLE 1. ADDONS POPULARITY

| Addon Name | Popularity % |
|---|---|
| Neptune Rising | 44 |
| Placenta | 23 |
| Genesis Reborn | 7 |
| Covenant | 5 |
| Incursion | 6 |
| Dog's Bollocks | 4 |
| Uranaus | 1 |
| Maverick | 2 |
| Other | 7 |

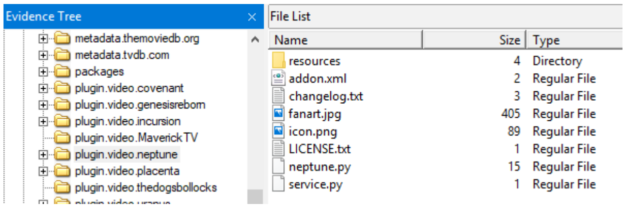
The SD card was removed from the Raspberry Pi and a raw image created using dd with hashes generated for integrity. The forensic image was analysed using Autopsy and FTK Imager.

## 4.2. Local Data Analysis

OSMC is a highly functional Linux OS. It has a similar tree structure to other Linux systems. Within the user's home folder there is a hidden .kodi folder. This directory contains the addons subfolder which holds a list of repository addons and video addons associated with the device under examination. It also contains two session log files; one is a current logfile active since the latest reboot and the other is an inactive logfile from the previous reboot. The logging available is customisable and can be found at `.kodi/temp/kodi.log` and at `.kodi/temp/kodi.old.log`. The logs take the format of Timestamp, Thread ID, FreeMem, Severity Level and Message. Severity levels are broken into Debug, Info, Notice, Warning, Error and Fatal.

Investigation of these addons reveal a common core file structure comprising of .xml, python, .txt and image files as can be seen in Figure 2. These files reveal the following information

- The file *addon.xml* is present for every addon. It comprises of several fields such as `<extension point="xbmc.addon.metadata">` that describes the addon to the user. Other fields reference any required dependencies, credits and version information.



Evidence Tree

- metadata.themoviedb.org
- metadata.tvdb.com
- packages
- plugin.video.covenant
- plugin.video.genesisrebom
- plugin.video.incursion
- plugin.video.MaverickTV
- plugin.video.neptune
- plugin.video.placenta
- plugin.video.thedogsbollocks

File List

| Name | Size | Type |
|---|---|---|
| resources | 4 | Directory |
| addon.xml | 2 | Regular File |
| changelog.txt | 3 | Regular File |
| fanart.jpg | 405 | Regular File |
| icon.png | 89 | Regular File |
| LICENSE.txt | 1 | Regular File |
| neptune.py | 15 | Regular File |
| service.py | 1 | Regular File |

Figure 2. Neptune Rising File Structure

- The files *addon.py* is the Python code that for the addon. The name of this file is usually defind in addon.xml.
- The *resources/* subdirectory stores files used by the addon that don't need to be stored in the root directory such as software libraries and translations. Since Kodi version 17, called Krypton, images are also stored in this location.
- The file *License.txt* file contains the text of the software license applied to the addon [19].

## 4.3. Local Data Results

Two types of addon were examined, repository addons and video addons. Repository addons have a smaller folder structure. They are made up of an addon.xml file and an image file. The addon.xml file contains links to the files needed to install and maintain the addons. These files tend to be stored in the GitHub cloud. A listing of the installed repositories can also be found in `.kodi/userdata/sources.xml`. The video addons have a larger folder structure more consistent with the list above. The folder structure of the Neptune Rising addon can be seen in figure 2.

## 4.4. GitHub Repositories

Each of these repository folders contains an addon.xml file which describes the repository. It has an `<extension point="xbmc.addon.repository" name="Official XBMC.org Add-on Repository">` tag which defines it as a repository addon and points to the cloud location of the repository. From here the plugin code for a video or audio streaming addon can be downloaded and installed on the device. Since the TVaddons repository server was taken offline in 2017 many repositories have moved to GitHub. This can be seen through examination of the `<info> <checksum> and <datadir>` tags visible in the repository's addon.xml file. These linking an addon to its GitHub storage account. The primary and secondary repositories associated with the addons can be seen in table 2. These all link to GitHub with the exception of Covenant's aeom repository which has been abandoned.

## 5. Cloud

GitHub is a cloud based development platform which allows for project management and version control of com-

TABLE 2. ADDONS AND THEIR ASSOCIATED REPOSITORIES

| Addon Name | Primary Repository | Secondary Repository | GitHub Storage |
|---|---|---|---|
| Neptune Rising | mrblamo (blamo repo) | dangre | Yes |
| Placenta | mrblamo | dangre | Yes |
| Genesis Reborn | jesusboxrepo | null | Yes |
| Covenant | xvbmc | aeom | Yes |
| Incursion | addons4kodi | null | Yes |
| Dog's Bollocks | mavrepo | supremacy | Yes |
| Uranaus | mrblamo (griffin repo) | null | Yes |
| Maverick | mavrepo | null | Yes |

puter code by individuals or among teams of people. People can be owners of repositories, collaborators, followers or can be followed by repository owners. Repositories can be public or private. Using the GraphQL API information on these addon authors and their networks can be gathered.

## 5.1. Cloud Data Collection

As Facebook transitioned to mobile devices it found that their systems provided users with an unsatisfactory experience. In 2012 they redesigned how they dealt with data and designed a new query language where data was viewed as nodes and the relationships between these nodes as edges. This query language was named GraphQL and was released as a draft standard in 2015. Since then it has become very popular with many cloud providers moving away from technologies such as REST and instead implementing their own Graph API. In order to do this a schema must be defined for data that resides in the cloud. Queries may then be issued to the cloud to gather information on pieces of data and their relationships with in that cloud platform.

## 5.2. Cloud Data Analysis

GraphQL was chosen for GitHub API V4. Using the schema a query was built about addon repository owners. In order to execute the request an authentication token for GitHub must be generated and passed with the query. The information collected on these GitHub users included name, url, createdAt, location, viewerIsFollowing, viewerCanFollow, updatedAt, bio, id, email, followers, followedBy. The information collected on the repositories id, name, description, parent, isFork, updatedAt, commitComments, forkCount, forks, downloadCount, releases, pullRequests, projects, mentionableUsers, milestones, labels, collaborators, totalCount, assignableUsers.

Each of the addon owners repositories were also examined. The query returned whether or not the repository was a parent, a fork, a count of forks, when it was last updated, any commit comments, pull requests and collaborators. A sample of the output from this query can be seen in Figure 4.

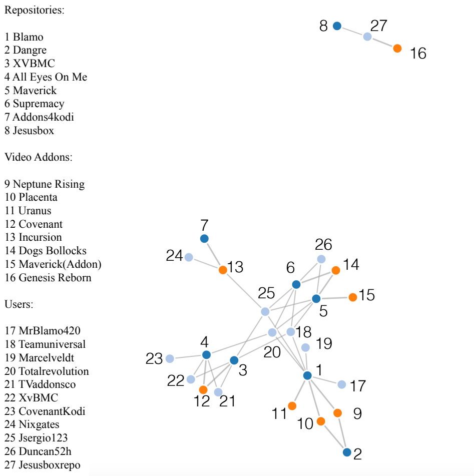
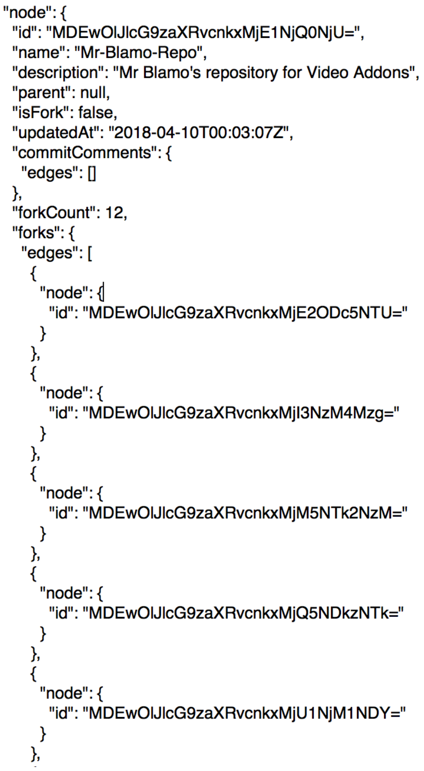


Figure 3. Graph of Relationships between Addons, Repositories and Distributors

## 5.3. Cloud Results

Data was successfully returned on the GitHub users identified and their associated repositories. The id data for each node is base 64 encoded and translates to the format of `<value><node-type><value>`. Examples include the user node `MDQ6VXNlcjcxOTgyNDk=` which represents `04:User7198249` and the repository node `MDEwOlJlcG9zaXRvcnk2MTkwODYxNQ==` which decodes to `010:Repository61908615`. These owners have repositories of varying sizes with the smallest hosting just one addon. A graphical representation of the relationships between addon distributors, addon repositories and video addons can be seen in Figure 3. The nodes of the repositories are 1-8, the video addons are 9-16 and the GitHub users are 17-27. The JesusBox repository (node 8) owned by Jesusboxrepo (node 27) and hosting Genesis Reborn (node 16) is independent from the other addons. Links can be seen with all the other addons. High edge counts from users to video addons indicate the reuse of their code in different addons. Examples of this are nodes 18, 20 and 25. Nodes 9-16 with more than one link indicates multiple distributors of a video addon.

There are a variety of roles in the Kodi community. Addon User is a normal user that installs and uses addons for streaming content. These can be further subdivided into legitimate and illegal users depending on whether the addons are streaming sources that infringe on copyright. Addon Authors are authors of Kodi addon code with a GitHub user profile. In some instances authors have written libraries such as resolvers or sounds which are reused in many Kodi addons. Addon Distributors are GitHub members hosting addon code. These distributors tend to host several video addons. Some video addons are hosted by multiple different distributors. Relationships exist between addon distributors as can be seen from querying a distributors followers and following lists and through repositories in Figure 3.



```
"node": {
  "id": "MDEwOlJlcG9zaXRvcnkxMjE1NjQ0NjU=",
  "name": "Mr-Blamo-Repo",
  "description": "Mr Blamo's repository for Video Addons",
  "parent": null,
  "isFork": false,
  "updatedAt": "2018-04-10T00:03:07Z",
  "commitComments": {
    "edges": []
  },
  "forkCount": 12,
  "forks": {
    "edges": [
      {
        "node": {
          "id": "MDEwOlJlcG9zaXRvcnkxMjE2ODc5NTU="
        }
      },
      {
        "node": {
          "id": "MDEwOlJlcG9zaXRvcnkxMjI3NzM4Mzg="
        }
      },
      {
        "node": {
          "id": "MDEwOlJlcG9zaXRvcnkxMjM5NTk2NzM="
        }
      },
      {
        "node": {
          "id": "MDEwOlJlcG9zaXRvcnkxMjQ5NDkzNTk="
        }
      },
      {
        "node": {
          "id": "MDEwOlJlcG9zaXRvcnkxMjU1NjM1NDY="
        }
      },
```

Figure 4. Sample .JSON output from Repository Query

Forking of repositories can be identified. Many new addons are forks of older addons which are no longer supported by authors. The level of activity on a repository can be seen through the number of commits and the numbers contributing to the repository. Download count can indicate the level of user adoption of a particular addon. A timeline of the development, what was added or removed, when this occurred and the handle of the GitHub user can be established. The output from this can be seen in the .JSON data in Figure 4.

Covenant is one of the best known video addons for Kodi and was part of the Colossus repository. The login name of the associated GitHub user is XvBMC according to the online sources listed earlier. A GraphQL query of this user states it ”could not resolve a user with the login of XvBMC”. Traversing the XvBMC GitHub account manually reveals 2 repositories. Respoitory.xvbmc appears to have been forked forty five times and hosts many different scripts and addons with in the repository. Two folders of interest are plugin.video.covenant and Dependencies. Addon.xml of plugin.video.covenant indicates the hosted version is 1.1.30 and is dependent on script.module.covenant, script.covenant.artwork version=1.0.0, script.covenant.metadata version 1.0.0, script.module.urlresolver version 3.0.0, script.module.requests and script.module.metahandler. The Dependencies folder contains several scripts including script.module.urlresolver and script.module.resolveurl.

The main contributor to the XvBMC repositories is a user with the login of EPiC-APOC. A GraphQL query of this user returns the username XvBMC and shows 3 repositories, the first named repository.xvbmc and the description ”XvBMC Nederlands forked”, the second named shares and the description ”that’s for me to know and you to find out” and the last is a fork of the second repository found in XvBMC Nederlands.

Further querying of GitHub for repositories showing covenant returns an account with login covenantkodi. There are seven repositories associated with this account with each providing a clear description. These can be seen in Table 3. The addon.xml file of the repository plugin.video.covenant indicates that this is a newer version, Covenant 1.1.34, than is being distributed by XvBMC. The addon.xml file in repository.colossus/plugin.video.covenant also indicates version 1.1.34. Though it was abandoned in November 2017 it is still being updated as of May 2018. However the updated version is not being distributed through XvBMC Nederlands at this time. Figure 3 shows the relationship between user covenantkodi (23), repository all eyes on me (4), user XvBMC (22), repository XVBMC and the video addon Covenant (12).

TABLE 3. STRUCTURE OF THE COVENANTKODI REPOSITORY

| Repository Name | isFork | fork Count | Description |
|---|---|---|---|
| plugin.video.covenant | false | 31 | Covenant Kodi Addon Development |
| repository.colossus | false | 47 | Colossus Repository for Kodi Addons |
| script.covenant.artwork | false | 10 | Covenant Artwork Development |
| script.covenant.metadata | false | 10 | Covenant Metadata Development |
| script.module.covenant | false | 16 | Covenant Module Development |
| script.module. metahandler | true | 0 | Metahandler Dependency Development for Kodi Addons |
| script.module. urlresolver | true | 9 | URLResolver Dependency Development for Kodi Addons |

The only two repositories present in covenenantkodi and which are not forks are script.module.metahandler and script.module.urlresolver. These modules are known as dependencies. They are needed by the video addons to support certain parts of the streaming process. Script.module.metahandler scrapes metadata from online services such as the Internet Movie Database (IMDB) and the Television Database (TVDB). Script.module.urlresolver takes the links which have been scraped from cyberlockers by the video addon and converts them into mediafiles which can be played by Kodi. The urlresolver script used here was forked from the account anxdpainc.

The anxdpanic urlresolver script was forked 31 times. Its description read that it was itself a ”Fork of Eldorado’s and Tknorris’s script.module.urlresolver”. However it does not have a parent node and isFork returns false. A query of the GitHub login Eldorado does not list script.module.urlresolver nor does a query of the the Tknorris GitHub account. Another fork of urlresolver called resolveurl is also present in the XvBMC Nederlands Repository.

## 6. Conclusion

Kodi has been around in various forms since 2003. Though an official figure for adoption cannot be found it would appear that there may be approximately 39 million regular users as of 2017. These users may be categorised as Addon users though it is difficult to break them down into legal or illegal addon users with estimates predicting that just over two thirds use addons for piracy. Other types of user are the authors of addon software who upload their code to the cloud and the addon distrubutors that manage how addon users get access to this code.

Examining a device can give an investigator a list of all installed addons and reveal where these were installed from. This links the device to the addon distributor on GitHub. Relationships exist between addon distributors as can be seen from querying a distributors followers and following lists. The level of activity on a repository can be seen through the number of commits. Download count can indicate the level of user adoption of a particular addon. Even though addons are publicly announced as being abandoned it appears they are still being developed. However the distributors are not releasing the newer version. Many new addons are forks of older addons which are no longer supported by authors. The forking of repositories can be identified and tracked using GraphQL. This use of GraphQL as an investigative tool gives insight into how these networks are organised and collaborate.

## 7. Future Work

Future work of this project focuses on applying data mining techniques for profiling and social network analysis of these addon distribution networks using the JSON GitHub data returned from the GraphQL queries. Further examination and analysis of local device data needs investigation across a range of devices. There are issues around the acquisition of data from some devices. It is also planned to investigate the relationships with these addons and the cyberlockers providing illegal streams. Addon python code needs analysis to see what it is executing and to identify issues which may leave users vulnerable to attack.

## References

[1] K. K. R. Choo and C. Esposito and A. Castiglione. *Evidence and Forensics in the Cloud: Challenges and Future Research Directions*, IEEE Journal of Cloud Computing, Volume 4 Issue 3, pages 14-19, 2017

[2] Godlovitch et al. *Over-the-Top (OTTs) players: Market dynamics and policy challenges*, European Parliament Directorate General for Internal Policies, Policy Department A: Economic and Scientific Poilcy IP/A/IMCO/FWC/2013046/ December 2015, http://www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf

[3] A. Sulleyman, *Most Kodi Users Need To Be Stopped From Using Illegal Addons To Watch Free Film and TV Streams, Says MPAA*, November 2017, https://www.independent.co.uk/life-style/gadgets-and-tech/news/kodi-addons-free-film-streams-tv-shows-online-live-football-mpaa-ne\\il-fried-a8040806.html

[4] G. Lynch, *7 out of 10 Kodi users are pirates, say Hollywood copyright overlords*, November 2017, https://www.techradar.com/news/7-out-of-10-kodi-users-are-pirates-say-hollywood-copyright-overlords

[5] TVaddons, *Kodi Addon Users: Impressive Numbers for January 2018 (Active Users)*, January 2018, https://www.tvaddons.co/statistics-january-2018/

[6] Europol, *Oone of Europe's Biggest Illegal IPTV Distributors Dismantled*, April 2017. https://www.europol.europa.eu/newsroom/news/one-of-europ's-biggest-illegal-iptv-distributors-dismantled

[7] B. Martini, Q. Do and K. K. R. Choo, *Mobile cloud forensics: An analysis of seven popular Android apps*. In Ko R and Choo K-K R, editors, Cloud Security Ecosystem, pp. 309 -345, Syngress, an Imprint of Elsevier, 2015

[8] H. Chung, J. Park, S. Lee, C. Kang, Digital forensic investigation of cloud storage services, Digital Investigation, Volume 9 Issue 2 Pages 81-95, Available at http://dx.doi.org/10.1016/j.diin.2012.05.015, 2012

[9] F. Chatziasimidis and I. Stamelos, *Data collection and analysis of GitHub repositories and users*, 6th International Conference on Information, Intelligence, Systems and Applications (IISA), 2015.

[10] I. Sutherland, K. Xynos, H. Read, A. Jones, T. Drange, *A forensic overview of the LG Smart TV*, in the Proceedings of the 12th Australian Digital Forensics Conference 2014

[11] A. Boztas, R. Riethoven and M. Roeloffs, *Smart TV Forensics - Digital Traces On Televisions*, From the proceedings of The Digital Forensic Research Conference, DFRWS 2015 EU Dublin, Ireland (Mar 23rd- 26th)

[12] J. Farina, M. Scanlon, N. Le-Khac, M-Tahar Kechadi, *Overview of the Forensic Investigation of Cloud Services*, in the 10th International Conference on Availability, Reliability and Security (ARES 2015) 2015

[13] D. Lillis, B. Becker, T. O'Sullivan, M. Scanlon",*Current Challenges and Future Research Areas for Digital Forensic Investigation*, 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016)

[14] K. Dreef, M. van der Reek, K. Schaper, M. Steinfort *Architecting Software to Keep the Lazy Ones On the Couch A Report On the Journey of Team Kodi*, http://delftswa.github.io/chapters/kodi/ April 23 2015

[15] G. Gousios, *The GHTorent dataset and tool suite*, 10th Working Conference on Mining Software Repositories (MSR), San Francisco, CA, 2013.

[16] NIST, *CVE-2016-2230*, 2016. https://nvd.nist.gov/vuln/detail/CVE-2016-2230

[17] NIST, *CVE-2017-6445*, 2017. https://nvd.nist.gov/vuln/detail/CVE-2017-6445

[18] Roku, *Devleoper Guide Debugging you Application*, 2018. https://sdkdocs.roku.com/display/sdkdoc/Debugging+Your+Application\\#DebuggingYourApplication\-Debugports

[19] Kodi Wiki, Kodi Addon Structure, 2018. https://kodi.wiki/view/Add-on_structure

[20] GitHub Graph API V4, 2018. https://developer.github.com/v4/

[21] Top Kodi Addons April 2018. http://www.wirelesshack.org/top-best-working-kodi-video-add-ons.html

[22] 115 Best Kodi Addons for *April 2018* 100% Working List for Krypton 17.6. https://www.vpnranks.com/best-kodi-addons/

[23] Best Working Kodi Addons List Download for Kodi 17.6 April 2018 https://www.kodiinfopark.com

[24] Top 10 Best Kodi Addons For Firestick & Android April 2018 https://mykodiaddons.com/best-kodi-addons-2018/

[25] 150 Best Kodi Addons for Krypton 17.6 April 2018 https://www.kodivpn.co/how-to-install-exodus-on-kodi/