UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
FORT LAUDERDALE DIVISION

MALIBU MEDIA, LLC, Plaintiff, v. ROBERT DARE, Defendant.	)	Civil Action No. 0:14-cv-61957-JIC

DEFENDANT'S MOTION FOR SUMMARY JUDGMENT WITH INCORPORATED MEMORANDUM OF LAW

COMES NOW Defendant, ROBERT DARE, by and through his undersigned counsel, pursuant to Rule 56, Federal Rules of Civil Procedure, and hereby moves for summary judgment as a matter of law on Plaintiff's claims in the Amended Complaint (Doc. 8).

I. Introduction & Procedural History

Plaintiff originally brought this case against an anonymous "John Doe" after alleging that its investigator determined that someone using IP address 98.249.146.169 downloaded Plaintiff's copyrighted motion pictures. After seeking leave of court (Doc. 5), Plaintiff sent a subpoena on Comcast, the Internet Service Provider who had issued IP address 98.249.146.169. A copy of the subpoena, which Plaintiff produced through discovery, is attached hereto as Exhibit "1."

The subpoena asked Comcast for the name and address of the Comcast customer who subscribed to IP address 98.249.146.169 on June 8, 2014, at the exact time of 00:13:41 UTC. According to documents also received from Plaintiff through discovery, Comcast responded with a letter identifying Defendant, Robert Dare, as the individual who subscribed to IP address 98.249.146.169 on June 8, 2014, at 00:13:41 GMT. Exhibit "2."

On December 8, 2014, Plaintiff amended its complaint (Doc. 8). Therein, it named Robert Dare specifically as Defendant and alleged that he downloaded, via the BitTorrent protocol, 17 individual video files at 17 distinct and very specific times ranging from March 15, 2014, at 10:31:45 UTC, to June 8, 2014, at 00:13:41 UTC. (Doc. 8-1 (listing all specific times).)

On October 13, 2015, the very day before the (extended) discovery period closed, Plaintiff conducted depositions of Defendant and of Defendant's wife, Cecilia Romero. Plaintiff did not ask questions regarding Defendant's whereabouts at the 17 distinct and very specific

times listed at Doc. 8-1. During his deposition, Defendant denied ever downloading Plaintiff's videos and said that, during the times of the alleged downloads of Plaintiff's videos, his router had not been password protected. Having an unprotected router would have enabled neighbors within range of the router's signal to access his Internet account and download Plaintiff's videos.

During Defendant's deposition, Plaintiff did not ask about the specific video titles listed at Doc. 8-1. Rather, Plaintiff focused its questioning on two areas: (1) whether Defendant had heard of any of the files listed in Plaintiff's "additional evidence" list (referenced at Doc. 8 ¶¶ 24-27) and (2) any information that Plaintiff could use to accuse Defendant of having lied, inadvertently or otherwise, or committed some discovery violation. For the latter, Plaintiff focused primarily on a computer Defendant had not used since about 2013, and therefore had not disclosed in his discovery responses (which had asked for computers used within a later time frame). The day after the deposition, Plaintiff filed a motion to extend the discovery deadline and to compel Defendant to give Plaintiff his computer (Doc. 69); therein, Plaintiff (wrongfully) accused Defendant of perjury. That motion was denied (Doc. 71).

The reason Plaintiff focused so strongly on trying to catch Defendant in some sort of a discovery violation or perjury is because doing so would be the only way Plaintiff has a chance of obtaining any sort of award against Defendant.

Plaintiff had an agreed discovery period, plus an extended period (pursuant to Doc. 55) to conduct discovery to prove that Defendant downloaded Plaintiff's 17 specific video files at the 17 very specific dates and times listed at Doc. 8-1. However, after finishing discovery, Plaintiff has obtained no actual evidence to prove, and cannot prove, that Defendant downloaded and distributed any of Plaintiff's 17 motion pictures. As such, Plaintiff cannot prove its case against Defendant, and summary judgment in Defendant's favor is proper.

II. Summary Judgment Evidence

This motion relies on the pleadings and documents in the court file as well as Defendant's answers to Plaintiff's first interrogatories (Doc. 54-2); Defendant's first requests for admissions (Exhibit "3")[1]; Declaration of Defendant, Robert Dare (Exhibit "4"); Plaintiff's response to Defendant's first request for production of documents (Exhibit "6"); the report of Defendant's expert witness, Tom Parker (Exhibit "7"); and Plaintiff's responses to Defendant's

[1] Defendant served requests for admission 1-39 (Exh. "3") on Plaintiff on August 3, 2015. As of the filing of this motion, Plaintiff has not provided any response or objections to these requests for admission. Accordingly, they are

interrogatories (Exhibit "8"). Pursuant to Local Rule 56.1, Defendant has also accompanied this motion with a statement of facts at Exhibit "9."

III. Standard

Under Rule 56(c), Federal Rules of Civil Procedure, a moving party is entitled to summary judgment "if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law."

The summary judgment analysis requires a two-part framework. *Celotex Corp. v. Catrett*, 477 U.S. 317 (1986). First, the movant carries the initial burden to "inform [ ] the ... court of the basis for its motion and [to] identify[ ] those portions of 'the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any,' which it believes demonstrate the absence of a genuine issue of material fact." *Id.* at 323.

Where, as in this case, the non-movant, Plaintiff, bears the burden of proof at trial:

> the moving party is not required to support its motion with affidavits or other similar material negating the opponent's claim in order to discharge this initial responsibility. Instead, the moving party simply may show [ ]-that is, point[ ] out to the district court-that there is **an absence of evidence to support the non-moving party's case**. Alternatively, the moving party may support its motion for summary judgment with affirmative evidence demonstrating that the non-moving party will be unable to prove its case at trial.

Fitzpatrick v. City of Atlanta, 2 F.3d 1112, 1115-16 (11th Cir. 1993) (emphasis added) (citing *U.S. v. Four Parcels of Real Property*, 941 F.2d 1428, 1437-38 (11th Cir. 1991). Summary judgment is particularly appropriate against a plaintiff who lacks affirmative evidence due to its failure to conduct adequate discovery. *See Ojeda v. Louisville Ladder, Inc.*, 410 Fed. Appx. 213, 215 (11th Cir. 2010).

Next, once the movant meets its burden, the burden shifts to the non-movant to demonstrate the existence of a genuine issue of material fact. The non-moving party must do more than simply show that there is some doubt as to the facts of the case. *Fitzpatrick* at 1116. The nonmoving party must go beyond the pleadings through the use of affidavits, depositions, answers to interrogatories and admissions on file, and designate specific facts showing that there is a genuine issue for trial. *Celotex Corp.*, 477 U.S. at 324. The evidence must be significantly probative to support the claims. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248–49 (1986).

IV. Analysis

Summary judgment is proper against Plaintiff because Plaintiff has absolutely no evidence to prove Defendant actually downloaded Plaintiff's films.

Plaintiff alleges Defendant used BitTorrent software on his computer to download a copy of Plaintiff's films, which was then allegedly uploaded to Plaintiff's investigator IPP International UG (Doc. 8 ¶¶ 17-22). "To make out a prima facie case of copyright infringement, a plaintiff must show that (1) it owns a valid copyright in the [work] and (2) defendant copied protected elements from the [work]." *Smith v. Casey*, 741 F.3d 1236, 1241 (11th Cir. 2014) (citations omitted). Demonstrating that Defendant himself downloaded, or made a copy of, Plaintiff's complete videos is therefore clearly a necessary element to prove Plaintiff's claims. As Plaintiff has no evidence to demonstrate that Defendant himself downloaded any of the videos alleged in the complaint, or that any videos were downloaded to completion, summary judgment should be entered in favor of Defendant.

A. Plaintiff has no evidence that IP address 98.249.146.169 was linked to Defendant for the alleged download timeframes

First, even though Plaintiff accuses Defendant of downloading 17 videos, Plaintiff has only tied Defendant to being the account holder of the IP address in question for one of the 17 alleged "hit" date and times. Therefore, Plaintiff has no evidence that the IP address in question was leased to Defendant on the "hit" date and times of the 16 other allegedly downloaded videos.

"IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet." *U.S. v. McCall*, 2:13-CR-144-MEF, 2014 WL 65738, at *13 (M.D. Ala. 2014). "IP addresses can change frequently due to their dynamic nature." *Bubble Gum Prod., LLC v. Does 1-80*, 2012 Copr. L. Dec. P 30292, 2012 WL 2953309 (S.D. Fla. 2012); *Call of the Wild Movie, LLC v Does 1-1,062*, 770 F.Supp. 2d 332, 357 (citing *Klimas v. Comcast Cable Commc'n, Inc.*, 465 F.3d 271, 275 (6th Cir. 2006) ("dynamic IP addresses constantly change and unless an IP address is correlated to some other information, such as Comcast's log of IP addresses assigned to its subscribers . . ., it does not identify any single subscriber by itself")). In *United States v. Vosburgh*,

> a witness from Comcast [Cable Communications] testified about IP addresses and the process by which Comcast responds to requests from law enforcement to match IP addresses to individual Comcast subscribers. He explained that Comcast's automated

> system assigns a unique IP number to each customer on a dynamic basis, and that the "lease period" for each IP address is approximately 6-8 days. At the expiration of that lease period, the assignment of an address to a particular computer may or may not be renewed. He further explained that Comcast can trace an IP address back to a particular customer's account, through IP assignment logs that go back 180 days.

602 F.3d 512, 523 (3d Cir. 2010).

On September 30, 2014, which was within 180 days of 06/08/2014, Plaintiff sent a third-party subpoena to Comcast (Exh. "1" and requested documents identifying the name, address, and telephone number of the Comcast customer assigned to IP address 98.249.146.169 on 06/08/2014 at 00:13:41 UTC. Exhibit "1." Although Plaintiff accuses Defendant of downloading *seventeen* separate videos at seventeen separate times (Doc. 8-1), the time on the Comcast subpoena, 06/08/2014 at 00:13:41 UTC, corresponds to only one alleged download: *Hot Orgasm*. *See* Doc. 8-1. The sixteen other videos were allegedly downloaded at entirely different times: *My Lover From Austria* was allegedly downloaded on 06/07/2014 at 23:35:38, *My Naughty Girl* on 06/07/2014 at 23:20:00, *Wild Things* on 05/03/2014 11:52:15, *Three Way is the Best Way* on 05/01/2014 01:59:07, *The Sleepover* on 05/01/2014 at 01:58:56, *Elle Hearts Girls* on 04/29/2014 at 07:13:21, *They Only Look Innocent* on 04/29/2014 at 03:16:50, *Triple Threat* on 04/29/2014 01:59:01, *Threes Company* on 04/29/2014 at 01:58:10, *No Turning Back Part #2* on 04/28/2014 at 02:32:02, *It Is A Fine Line* on 04/28/2014 at 01:59:33, *Group Sex* on 04/27/2014 at 02:32:54, *Just the Three of Us* on 03/15/2014 11:27:55, *Go Fish* on 03/15/2014 at 11:12:40, *Playing Dress Up* on 03/15/2014 at 10:42:25, and *All Oiled Up* on 03/15/2014 at 10:31:45. (Doc. 8-1.)

In response to Plaintiff's subpoena, Comcast submitted a document identifying the accountholder for the IP address 98.249.146.169 on 06/08/2014 at 00:13:41 GMT as Robert Dare. Exhibit "2." The subpoena response did not include any other date or time information.

As indicated in *Vosburgh*, Comcast assigns dynamic IP addresses. This means that, even if Plaintiff had irrefutable proof that IP address 98.249.146.169 was assigned to Robert Dare's Comcast account on 06/08/2014 at 00:13:41 UTC, such would not mean that said IP address was assigned to his account on any of the *other* alleged "hit" dates. Essentially, Plaintiff failed to obtain the identity of the Comcast customer who subscribed to IP address 98.249.146.169 at sixteen of the seventeen alleged "hit" dates.

Furthermore, even if the discovery period were still open, Plaintiff would not be able to obtain such information because well over 180 days have passed, which means Comcast has purged this information from its systems.

Plaintiff attempted to depose a representative of Comcast on the very last day of the extended discovery period, but was not able to do so. By Plaintiff's own admission, "**Without Comcast's testimony, Plaintiff cannot establish that the IP address which was used to infringe Plaintiff's copyrighted works was assigned to Defendant**." Pl 2d Mot. to Enlarge Disc'y Period, Doc. 69 at 2.

Assuming *arguendo* that Comcast's subpoena response would be admissible at trial, this remains a question of fact for only one of the 17 videos, *Hot Orgasm*, which was allegedly downloaded at 6/08/2014 at 00:13:41 UTC. Other than this one single video "hit" date/time, Plaintiff has no evidence, and cannot obtain any evidence, linking IP address 98.249.146.169 to Defendant during the sixteen separate occurrences other than 06/08/2014 at 00:13:41 UTC. As such, summary judgment should, at the very least, be granted in favor of Defendant for the allegations related to the sixteen separate alleged downloads that allegedly occurred on times other than 06/08/2014 at 00:13:41 UTC.

B. Plaintiff has no evidence that Defendant downloaded Plaintiff's videos

Next, after a complete discovery period, Plaintiff, which has the burden of proof, has no actual or direct evidence that Defendant downloaded *Hot Orgasm* or any other of Plaintiff's alleged videos.[2] Defendant has strongly denied having downloaded Plaintiff's videos. Plaintiff's entire case, therefore, is a hasty generalization based on speculation. Plaintiff has no admission from Defendant, no witness to the download, and no forensic evidence, yet has jumped to the unsupported — and wrong — conclusion that Defendant must be liable.

1. Plaintiff relies purely on speculation

First, Plaintiff's entire evidence is speculation and not even a scintilla of evidence. In Defendant's Interrogatory No. 13, Defendant asked: "Did Defendant download the entire torrent files to completion? If your answer is "yes," please explain any and all facts on which you rely to arrive at that conclusion." Exh. "8" at 5. Plaintiff's answer is pure speculation: "Yes. Obtaining

[2] *See* Exh. "3" at 5 # 1, Defendant's requests for admissions to Plaintiff, asking, "You have no evidence to tie Defendant directly to the alleged downloads." Plaintiff failed to respond or object to this request for admission; accordingly, it is deemed admitted. Fed. R. Civ. P. 36(a)(3).

a complete copy of a computer file is the purpose of using BitTorrent. And, Defendant obviously obtains complete files because he uses BitTorrent all of the time." Exh. "8" at 6. In reality, however, Plaintiff has *no* facts to show that Defendant downloaded Plaintiff's videos.

In another interrogatory, No. 18, Defendant asked, "Do you have any evidence, other than an IP Address, to prove that Defendant, ROBERT DARE, and no one else committed the infringements alleged in the amended complaint? If so, please identify, with particularity and to completion, any and all such evidence." Exh. "8" at 9. Although Plaintiff's answer spans two pages, like its answer to No. 13, it is, in reality, nothing but speculation and fails to include any actual evidence. As such is all of the "evidence" that Plaintiff has, it is not enough. First, Plaintiff references that its investigator discovered that "an individual" had used the subject IP address to download seventeen (17) of Plaintiff's videos "between March 15, 2014 and June 8, 2014." Then, Plaintiff answers, in a very conclusory fashion, that "Plaintiff considers Defendant to be a serial infringer of its copyrighted works."

Plaintiff places much weight on the list it titles the "Additional Evidence" then states, again in conclusory fashion, "that Defendant's IP address has continually infringed third-party copyrighted works such as mainstream movies and television shows." Exh. "8" at 9-10. Again, however, Plaintiff only indicates that the "Additional Evidence" is tied to an IP address, not a person.

Plaintiff then speculates that, because Defendant has a strong employment history working with computers, including as a Java developer, makes him liable. *Id*. However, BitTorrent use does not require any particular sophistication, experience, or education. It is so simple that "[e]ven a child can do it." Exh. "7" at 8.

Plaintiff then speculates that because Defendant's wifi was password protected *in 2013* when the "Additional Evidence" files were allegedly downloaded, that Defendant must be the downloader. Plaintiff fails to take into account that, even at the time that his Internet had a password, Defendant was not the only individual who used his Internet account. Additionally, despite completing discovery, Plaintiff has no more evidence than speculation that Defendant actually downloaded any of the items on the Additional Evidence list. Moreover, *this case is not about the "Additional Evidence"* or events that occurred in 2013. It is about *Plaintiff's videos* that were allegedly downloaded in 2014. Even assuming, *arguendo*, if IP address 98.249.146.169 did belong to Defendant in 2013 and Defendant did download every single item

on the "Additional Evidence" (which he did not), Plaintiff *still* would have no evidence beyond speculation that Defendant downloaded any of *Plaintiff's* videos in 2014.

Plaintiff further speculates that because its investigator concluded that the works had been downloaded using software called "Transmission" that Defendant must be the downloader because Defendant used a Mac and had previously used that client. However, Transmission is one of the Top 5 BitTorrent clients and is widely used.[3] This speculation is almost like if a Plaintiff found an empty discarded Monster Energy drink can at the scene of a car accident and, without analyzing tire tracks or other forensics, concluded that a random individual who likes Monster Energy must have caused the accident. Such is the logical fallacy of jumping to conclusions. Moreover, Plaintiff speaks of BitTorrent as if it were rare; however, BitTorrent "is one of the most popular ways internet subscribers transfer data from one device (a peer) to another (peer)." *Voltage Pictures, LLC v. Does 1-31*, 291 F.R.D. 690, 692 (S.D. Ga. 2013) (citation omitted). It was estimated in 2013 that "BitTorrent was responsible for 3.35% of all worldwide bandwidth."[4]

All of this speculation does not even amount to a *scintilla* of evidence; however, even if it did amount to a *scintilla*, that would be insufficient. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 252 (1986) ("The mere existence of a scintilla of evidence in support of the plaintiff's position will be insufficient; there must be evidence on which the jury could reasonably find for the plaintiff"); *see also Walker v. Darby*, 911 F.2d 1573, 1577 (11th Cir. 1990). Because Plaintiff lacks any *significantly probative* evidence to support its claims, however, its speculation — and its unsupported, generalized conclusions — are insufficient. *Anderson, Inc.*, 477 U.S. 248–49 (1986).

2. Plaintiff has no admission from Defendant

When it comes to concrete evidence, however, Plaintiff has nothing. One way to prove a copy had been made could have possibly been for Plaintiff to obtain an admission. However, Plaintiff asked Defendant, "have you ever searched for X-Art, Malibu Media, or torrent files on the internet?" and Defendant responded, "No." (Doc. 54-2 at 22-23 (Rog 15)). Furthermore,

[3] *E.g.*, P&P & File Sharing Software for Mac, http://download.cnet.com/mac/p2p-file-sharing-software/?sort=downloadCount~desc (Listing Transmission as the top-rated client and showing it to have had 355,429 downloads since July 2014); Alan Henry, *Five Best BitTorrent Clients*, LIFEHACKER (May 17, 2015) http://lifehacker.com/5813348/five-best-bittorrent-applications; Manuel Jose, *Top 5 Bit Torrent Clients For Ubuntu*, TECHDRIVEIN, http://www.techdrivein.com/2011/01/top-5-bit-torrent-clients-for-ubuntu.html (2011).

[4] Wikipedia: BitTorrent https://en.wikipedia.org/wiki/BitTorrent (citation omittied).

Defendant stands by his denial of liability. Exh. "4," Declaration of Robert Dare. Therefore, Defendant has denied liability, and Plaintiff has not obtained an admission.

3. Plaintiff has no witness who saw Defendant perform the downloads

Another way to prove a copy was made could be through testimony of a witness who saw or otherwise observed Defendant (meaning the individual, not the IP address) download the videos. Plaintiff deposed Defendant's wife, who did not provide such testimony. Plaintiff deposed neighbor who lives across the street from Defendant, and he attested to barely knowing who Defendant was and never seeing Defendant use a computer. Plaintiff did not depose anyone else. Plaintiff also never sent out any investigator to Defendant's home, or near it, to investigate Defendant or Defendant's internet connection on location. (Exh. 8 at 17, Rog 20.)

4. Plaintiff has no forensic or computer evidence linking Defendant to the downloads

A third way to prove a copy was made – based on Plaintiff's explanation of how BitTorrent works – could be to prove the videos had been downloaded onto a specific computer, then proving that Defendant used that computer at the relevant times.

In an attempt to obtain such information, Plaintiff sought from Defendant copies of documents resulting from a search of all computers Defendant used during the alleged download period for the titles of Plaintiff's works as listed in Exhibit B to the Amended Complaint as well as terms "X-Art," "Malibu Media," or "torrent." Of the computers Defendant had used within the alleged download period, Defendant had only iPhones and iPads in his possession, custody, or control. He brought these devices to NextDoorGeeks, LLC to have the requested search performed. The search revealed no documents. Exh. "4" at ¶¶ 5-7.

The only other computer Defendant had used at his home within the subject download period was a work-issued computer that Defendant had returned to his former employer, OpenPeak, in August 2014. (Doc. 54-2 at 9.) On or about September 22, 2015, Plaintiff served OpenPeak with a subpoena asking for a clone of the hard drive. On or about October 2, 2015, OpenPeak responded and said that the computer had been disposed of due to damage and was therefore unavailable. Exhibit "5," response from OpeanPeak.

Accordingly, Plaintiff has failed to obtain any evidence that any of the alleged videos were downloaded onto any of Defendant's computer devices.[5]

Therefore, without any actual evidence demonstrating that Defendant downloaded Plaintiff's videos — no admission, no witness, no computer evidence — Plaintiff cannot prove that Defendant copied Plaintiff's videos via BitTorrent as alleged in the complaint. Therefore, Plaintiff cannot prove its claims for copyright infringement, and summary judgment should be granted for Defendant.

C. Defendant was running an open guest network that was accessible by neighbors and was not password protected

Because Defendant's Internet was accessible by neighbors via an unprotected Wi-Fi, if Plaintiff's videos were downloaded from Defendant's Internet account, the downloader could have been — and probably was — a neighbor.

1. Defendant's Wi-Fi had an open guest network

In discovery, Plaintiff asked Defendant to identify each wireless router and modem used in his home and the duration during which it was password protected. (Doc. 54-2 at 10-11 (Rog 5).) Defendant identified a Netgear N600 wireless router and said that he himself had installed it. He further explained:

> The unit, along with cable modem was deactivated between December 2013 and February 2014 due to an extended family trip outside of the country. Upon return in February of 2014, we had many guests coming to visit and I removed the password for the 2.4 Ghz band to make it a guest network. Once I received notice from Comcast regarding this lawsuit, I replaced the password, changed the SSID, and disabled SSID broadcast.

Doc. 54-2 at 11 (Rog 5).

2. Defendant's next door neighbor were so close they shared a wall with Defendant

Plaintiff also asked Defendant to identify each person to whom he provided with access to his wireless router during the last two years. (Doc. 54-2 at 13 (Rog 7).) Defendant identified

[5] Although Plaintiff owned another, older computer, which had been sitting in his closet, he did not use this computer or even turn it on during time period of the alleged downloads. Therefore, this computer is not relevant, and no copies of Plaintiff's videos can be obtained from it. *See also* Exh. 4 ¶ 8, declaration of Robert Dare.

himself and his wife, plus at least four specific guests plus "unknown persons (neighbors and their guests) within the range of the routers" as having access to the wireless router during the past two years. (Doc. 54-2 at 13-14 (Rog 7).)

Throughout and since the time of the alleged downloads (March through June 2014), Defendant has resided in a multi-family condominium structure with six units to his building. Within the building, Defendant's unit is No. 3, and both left and right sides of Defendant's unit share a wall with Units 2 and 4.

The condominium is built with all six units in a row, all facing the street, as such:

Unit 1	**Unit 2**	**Unit 3** Defendant, his wife, and two infant children	**Unit 4**	**Unit 5**	**Unit 6**
EAST ARAGON BOULEVARD					

As Defendant explains in his declaration (Exh. 4), during the time of the alleged downloads, Defendant's immediate next-door neighbors were the residents of Units 2 and 4. The couple who resided in Unit 2 in 2014 moved out in early 2015, and Defendant did not maintain contact with them. The gentleman was a mechanic, and he sometimes worked on cars in the garage, while his girlfriend would sit with her laptop in the garage. Various other people reside in the other units. In Unit 4, for instance, so many people have come and gone that Defendant is unsure as to who exactly resides there. In Unit 1, a family resides; in Unit 5 during 2014 a young couple lived there; and, in Unit 6, a man and his wife have resided.

Although Plaintiff deposed a neighbor from across the street, Plaintiff did not depose any neighbors in the same building as Defendant, who would be the neighbors more likely to have accessed Defendant's signal.

3. Defendant's wifi signal extends beyond the walls of his condominium unit

Because Defendant lives in such close proximity to other neighbors, wifi signals pass through the walls. As Defendant explains in his declaration (Exh. 4), Defendant made observations to detect whether other wifi signals could be detected from within his own unit. While he was in his kitchen and living room, and upstairs (and not next to a window or open door), Defendant viewed the network preferences of his computer and noticed that at least 12

wifi signals other than his own were visible. These signals had not been generated from within Defendant's unit and came from neighbors. Therefore, the walls of Defendant's condominium structure are such that wifi signals can pass through them — including into Units 2 and 4, and possibly Units 1, 5, and 6.

Defendant still has installed in his home the same Netgear N600 wireless router that was installed during the alleged download period. In an effort to determine whether the signal from that router could be detected from outside the walls of his condominium unit, Defendant carried his laptop computer outside and took it to various access points in front of, beside, and behind his unit, and at each point examined his computer's network preferences. (Exh. 4.) Defendant observed that his his signal was accessible from various access points at all sides of his home, which indicates that the signal would also be accessible within the units directly adjacent to Defendant's home, with the very units with which Defendant shares walls. (Exh. 4.)

Defendant even went as far as to download an application called NetSpot, which is used to test Wi-Fi signal strengths. He then input the appropriate measurements into the application to detect the strength of his Wi-Fi from various access points. The wifi is measured in decibel-milliwatts, abbreviated "dBm." He made a screenshot of his unit as well as various access points, where he had walked around outside, and attached the screenshot to his declaration (Exh. "4.")

D. None of Plaintiff's trial evidence links Defendant to the downloads of Plaintiff's videos

Next, none of the evidence Plaintiff produced can connect the alleged downloads to Defendant anymore than it can connect them to any other person who had access to IP address 98.249.146.169.

> It is common today for people to use routers to share one internet connection between multiple computers, the subscriber associated with the IP address may not necessarily be the alleged infringer and instead could be the subscriber, a member of his or her family, an employee, invitee, neighbor or interloper. Therefore, the assumption that the person who pays for Internet access at a given location is the same individual who allegedly downloaded a single sexually explicit film is tenuous, and one that has grown more so over time.

Bubble Gum Prod's, 2012 Copr. L. Dec. P 30292 (quoting *In re BitTorrent Adult Film Copyright Infringement Cases,* 2012 WL 1570765, at *3 (E.D.N.Y. May 1, 2012) (internal quotations and citations omitted). "[A] viewable IP address may represent nothing more than a router or gateway through which other devices connect. These devices, which may be part of a large intranet, may have their own private IP addresses that are not visible to users of the Internet outside of the intranet to which the device is connected." *Malibu Media, LLC v. Doe*, 0:14-CV-60259-UU, 2014 WL 2615351, at *2, n. 2 (S.D. Fla. 2014).

1. Plaintiff's only evidence links the *IP address*, not Defendant, to the alleged downloads of Plaintiff's videos.

Plaintiff has no evidence, whatsoever, linking Defendant to the alleged downloading of its videos. Defendant propounded request for production number 39 on Plaintiff and therein asked for "true and correct copies of any and all documents, including investigation reports, you relied upon to conclude Defendant was the individual who infringed your works." Exh. "6" at 14. Plaintiff responded that it would "produce all documents it intends to use at trial which it will rely upon to conclude Defendant was the individual who infringed Plaintiff's works." Exh. "6" at 14. The core of these documents is an electronic document represented as a "PCAP" (or pocket capture) which, according to Plaintiff, represents the actual data from a pocket of traffic captured by Plaintiff's expert. Plaintiff produced one PCAP that corresponds to each of its videos allegedly downloaded. Plaintiff also produced copies of the corresponding .torrent files[6]; reports prepared by Plaintiff supposedly based on the data in the PCAPs; a list of names of third-party files that Plaintiff calls the "Additional Evidence"; TAR[7] files containing copies of the actual videos; and an excel spreadsheet called "MySQL Log" (and "Updated MySQL"), in which Plaintiff plugged in dates and times pulled from the PCAPs. Plaintiff also produced its Articles of Organization, its subpoena to Comcast, and Comcast's subpoena response.

The data files that Plaintiff produced that are related to Plaintiff's videos — the PCAPs and spreadsheets and reports based on them — identify only an IP address, 98.249.146.169, as allegedly downloading Plaintiff's films. They have no information or data that can identify a

[6] A "torrent" file contains metadata about the content to be distributed, such as the name, size, folder structure, cryptographic hash values, and information about where to look on the Internet for the actual pieces of the file. *See, e.g.*, *MCGIP, LLC v. Does 1–30*, No. 11 C 3680, 2011 WL 3501720, at *1 (N.D. Cal. Aug. 10, 2011) (quoting *Diabolic Video Prods., Inc. v. Does 1–2099*, No. 10 C 5865, 2011 WL 3100404, at *1 (N.D. Cal. May 31, 2011)).

[7] TAR files are named so after "tape archive." TAR is a format for archiving files, or merging several files into one. The format is usually for ease of file distribution.

specific computer or individual. *See, e.g.*, Exh. "7" at 8 ("none of Plaintiff's evidence presented shows which computer, if any, downloaded the videos in question").

It is well established that an IP address corresponds to a router, not a computer. "[T]he assumption that the person who pays for Internet access at a given location is the same individual who allegedly downloaded a single sexually explicit film is tenuous, and one that has grown more so over time." *Bubble Gum Prod's, LLC*, 2012 Copr. L. Dec. P 30292 (citation omitted); *see also* Exh. "7" at 7 ¶ H ("An IP address corresponds to a router, not a computer.") Here, Plaintiff's investigators did not detect any specific computer device. Exh. "7" at 7 ¶ H. Multiple computer devices can connect to one IP address. The router used by Defendant has a "Network Address Translation Firewall, which conceals behind it the devices that would be connected to the router. Therefore, none of Plaintiff's evidence presented shows which computer, if any, downloaded the videos in question." Exh. "7" at 7¶ H.

Therefore, Plaintiff only has gathered evidence to show that an IP address, not an individual, allegedly downloaded the videos. "None of Plaintiff's evidence presented shows which computer, if any, downloaded the video in question." Exh. "7," at 7 ¶ H. Therefore, even if Plaintiff could prove that the downloads were caused from Defendant's Internet account, Plaintiff still would not be able to prove that Defendant was the individual who downloaded its videos.

2. Plaintiff's "Additional Evidence" cannot link Defendant to the downloads of Plaintiff's videos

Furthermore, Plaintiff produced alleged "Additional Evidence" in this case, which is a list of alleged downloads from IP address 98.249.146.169 separate from Plaintiff's videos, and which appear to have been downloaded at various times and dates. *See* Doc. 8, ¶¶ 24-27.

As an initial matter, the "additional evidence" is only a list. It had "no accompanying PCAP data, no torrent file, no copy of the video, nor any other accompanying data." (Exh. "7" at 7.) Therefore, there is no way to tell that the items on the list actually are what they purport to be.

Plaintiff also produced an unauthenticated printout of a YouTube page allegedly corresponding to Robert Dare. However, this printout has no allegation of anything to do with Plaintiff's videos or Plaintiff's "X-Art" brand. The only reason Plaintiff produced it is because it indicates that Defendant allegedly "liked" a video of Beethoven's moonlight sonata, and that one

of the items on the "Additional Evidence" appears to be a copy of Beethoven's 5th Symphony. First, even if Defendant does like Beethoven, such would not be direct evidence that he used BitTorrent to downloaded Beethoven's "Symphony 5," which has been called the most famous piece of classical music of all time. Secondly, even, *arguendo*, if Defendant did download a Beethoven symphony via BitTorrent (which he did not), such has nothing to do with *Plaintiff's* pornographic videos. Plaintiff has not shown that its videos incorporate Beethoven classical music or that Beethoven has anything to do whatsoever with Plaintiff's pornography. Therefore, the document is wholly irrelevant and does nothing to prove Plaintiff's claims.

Other than the suggestion that Defendant may "like" Beethoven, Plaintiff has nothing, other than an IP address, to link the items on the "Additional Evidence" list to the same computer device or individual, or to link them to the downloading of Plaintiff's videos. Essentially, the items on the list could have been downloaded by any combination of individuals or computers accessing the router. To say that the videos logged on that list were all downloaded by the same individual, and that the same person who downloaded those items was the single individual who downloaded all 17 of Plaintiff's videos is like saying, by examining cash receipts, that a coffee bought at 7-Eleven on a Friday was bought by the same person who purchased a donut on Sunday because both items were purchased at the same 7-Eleven. The logged traffic related to the same IP address, but, where that IP address is accessed by multiple individuals, such traffic can no more accurately identify a downloader than a logged cash receipt at 7-Eleven, alone, would be to identify the cash purchaser of a donut.

"The additional evidence is not specific to one computer on IP address 98.249.146.169." (Exh. "3" at 8 RFA 30.) "The alleged downloads and/or the 'additional evidence' could have been downloaded from more than one computer connected to IP address 98.249.146.169." (Exh. "3" at 7, RFA 22.) "The additional evidence was downloaded from more than one computer connected to IP address 98.249.146.169." (Exh. "3" at 8 RFA 31.) In other words, assuming that the list represents files that were allegedly downloaded, part of the files on could have been downloaded by one person while other files were downloaded by another person accessing network. Or, the additional evidence could have been downloaded by one person why Plaintiff's videos could have been downloaded by someone else on the network. Because the computer device(s) that allegedly downloaded the files are not identified, there is nothing tying all of the downloads on the additional evidence to the same person, or, for that matter, all of the alleged downloads on the additional evidence and the alleged downloads of Plaintiff's works to the same

person. Regardless, Plaintiff has no evidence beyond speculation that Defendant is the individual who downloaded the additional evidence files. Therefore, even if, *arguendo*, Plaintiff could prove that Defendant downloaded all the videos on the list of additional evidence (which he did not), such proof would not prove that Defendant downloaded Plaintiff's completely unrelated and separate pornographic films on completely separate occasions.

As Plaintiff cannot provide any evidence that Defendant, himself, performed the downloads, nor any evidence that the same person who downloaded the additional evidence is the same person who downloaded Plaintiff's videos, the additional evidence cannot be used as evidence that Defendant downloaded Plaintiff's videos.

E. At best, Plaintiff only has evidence that an unusable piece of movie — and not an entire movie — was copied by a computer connected to IP address 98.249.146.169

Finally, *arguendo*, even if Plaintiff could somehow link the downloads of its videos directly to Defendant's computer (which it cannot), it still would not — without seeing full and complete files on Defendant's computer — be able to prove that Defendant downloaded full and complete files of Plaintiff's videos. Because there are no copies of Plaintiff's videos on Defendant's computer, Plaintiff cannot prove this case.

To establish copyright infringement, Plaintiff must demonstrate that the file transferred by IP address 98.249.146.169 is substantially similar to Plaintiff's work. *Arthur Rutenberg Corp. v. Dawney*, 647 F. Supp. 1214, 1216 (M.D. Fla. 1986). However, Plaintiff's data — in the form of a "PCAP" or "pocket capture" for each video — is "not representative of an entire video and does not contain sufficient data to show that an entire video was transferred." (Exh. "7" at 4.)

According to Plaintiff, "to distribute a large file, the BitTorrent protocol breaks a file into many small pieces called bits. Users then exchange these small bits among each other instead of attempting to distribute a much larger digital file." (Doc. 8, ¶ 12). "Each PCAP clearly shows the IP address distributing the BitTorrent piece (Defendant's IP address), the IP address receiving the BitTorrent piece (Excipio's IP address), [and] what was transmitted." Doc. 62-2 at 4 ¶ 20. For *Hot Orgasm*, file hash 91D22A6F66495928D68FE6EFE63FC676FD6AC763, for example, the associated PCAP file produced by Plaintiff has a file size of only 67KB and demonstrates that Plaintiff only detected Defendant's public IP address allegedly transferring *one piece* of a file as opposed to a whole movie. Exh. "7" at 4. According to the .tar file produced by Plaintiff, which is a copy of *Hot Orgasm* (but not allegedly downloaded from IP address 98.249.146.169),

the full video file of *Hot Orgasm* has a total file size of 441.2MB. *Id*. Comparatively speaking, Plaintiff's PCAP, which is Plaintiff's *only evidence* of recording any downloading of *Hot Orgasm* from IP address 98.249.146.169, is only 0.015% the size of the actual film. *Id*. Thus, Plaintiff only has evidence that a fragment of its video was downloaded from IP address 98.249.146.169.

Because the PCAP only includes data for one piece, it does not include enough data to correspond to an entire video file. For a torrent file to be viewable, it needs all of the torrent pieces. *See, e.g.*, Doc. 8, ¶ 13 ("After the infringer receives all of the bits of a digital media file, the infringer's BitTorrent client software reassembles the bits so that the file may be opened and utilized.") Furthermore, copying a single piece of a torrent is not the same thing as copying an entire video file. Exh. "7" at 5. For a movie to be watchable, it needs all the pieces. A movie file that is missing pieces will be disrupted based on how many pieces are missing. *Id*. Neither Plaintiff nor Defendant can view the "piece" or "bit" captured in the PCAP to determine what portion of Plaintiff's film it correlates to. It is possible that piece contains only a black screen as when the film fades in between frames, which would not be copyrightable, or that it is not viewable at all. Neither Plaintiff nor Defendant can know, from analyzing Plaintiff's data, what is contained in the fragment that was allegedly transferred by IP address 98.249.146.169, as shown by the PCAP, or whether it bears any substantial similarity to the actual copyrighted work. Any argument by Plaintiff that the transmission of a single piece of a video means that an entire video was downloaded is mere speculation relying on assumptions and generalizations.

Therefore, without being able to demonstrate that a computer connected to IP address 98.249.146.169 transferred all of the pieces of, and therefore, the entire video, Plaintiff cannot establish that that computer that connected to IP address 98.249.146.169 copied the film. *See, e.g., Malibu Media v. Doe*, 2015 WL 412855 (E.D. Pa. Feb. 2, 2015) (granting a motion for summary judgment in favor of Defendant because, even though Malibu Media had found what it purported to be a fragment of a video file on Defendant's computer, that it had "a complete failure of proof concerning an essential element of its claim").

Because, outside speculation, Plaintiff cannot prove anything more than the downloading of a mere fragment of a video file by a computer connected to IP address 98.249.146.169, and Plaintiff has no evidence to show whether that fragment is viewable, summary judgment should be granted in Defendant's favor.

V. Expenses and Attorney's Fees

Lastly, section 505 of the United States Code provides for an award of attorney fees as costs to the prevailing party in a copyright infringement action. *Arthur Rutenberg Corp. v. Dawney*, 647 F. Supp. 1214, 1216 (M.D. Fla. 1986) (citing 17 U.S.C. § 505). An award of attorney fees to the prevailing party in a copyright action is the rule rather than the exception. *Hunn v. Dan Wilson Homes, Inc.*, 789 F.3d 573 (5th Cir. 2002).

VI. Conclusion

First, Plaintiff cannot prove that Defendant was the subscriber of IP address 98.249.146.169 for all the dates and times that Plaintiff alleged its videos were downloaded. It only obtained evidence that Defendant subscribed to IP address 98.249.146.169 on the precise date and time of 06/08/2014 at 00:13:41 UTC, which was the alleged hit date for only one of Plaintiff's videos. Secondly, Plaintiff failed to obtain any evidence that Defendant downloaded its videos. It has no admission from Defendant, no eyewitness, and no forensic or computer evidence linking Defendant to the downloads. Furthermore, Plaintiff's own evidence does not connect Defendant specifically to the downloads; rather, it only links IP address 98.249.146.169, not any particular computer or individual, to the alleged downloads. Because Defendant was running an open guest network that neighbors could access by without a password during the alleged download period, evidence linking Defendant, and not just an IP address, is essential. Plaintiff's much touted "additional evidence" is not evidence of the downloading of Plaintiff's videos because it is a list of entirely different files allegedly downloaded at different times, and there is nothing linking such evidence to Defendant. Lastly, at best, Plaintiff's evidence indicates the copying of not an entire movie but rather a single, unusable fragment. As the evidence produced by Plaintiff and recovered by Plaintiff during discovery is not sufficient to support a claim of copyright infringement, summary judgment should be had in favor of Defendant.

WHEREFORE, Defendant, ROBERT DARE, pleads that this Honorable Court enter final summary judgment in favor of Defendant and award Defendant its costs, including attorney's fees, pursuant to 17 U.S.C. § 505, as prevailing party.

CERTIFICATE OF SERVICE

I hereby certify that on **October 20, 2015**, I filed electronically the foregoing with the Clerk of the Court via CM/ECF system which will notify electronically all parties.

Attorney for Plaintiffs:
Cynthia Conlin, P.A.
1643 Hillcrest Street
Orlando, Florida 32803-4809
Tel. 405-965-5519/Fax 405-545-4395
www.conlinpa.com

/s/ Cynthia Conlin, Esq.
[X] CYNTHIA CONLIN, ESQ.
Florida Bar No. 47012
Cynthia@cynthiaconlin.com
[ ] JENNIFER REED, ESQ.
Florida Bar No. 104986
Jennifer@cynthiaconlin.com
Secondary Email for Service:
Jeff@cynthiaconlin.com