

1 J. CHRISTOPHER LYNCH, WSBA #17462
JEFFREY R. SMITH, WSBA #37460
2 RHETT V. BARNEY, WSBA #44764
LEE & HAYES, PLLC
3 601 W. Riverside Avenue, Suite 1400
Spokane, WA 99201
4 Phone: (509) 324-9256
Fax: (509) 323-8979
5 Emails: chris@leehayes.com
jeffreys@leehayes.com
6 rhettb@leehayes.com

7 *Counsel for Defendant Ryan Lamberson*

8
9 **UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WASHINGTON**

10 ELF-MAN, LLC,

11 Plaintiff,

12 vs.

13 RYAN LAMBERSON,

14 Defendant.
15

No. 2:13-CV-00395-TOR

SUPPLEMENTAL DECLARATION
OF J. CHRISTOPHER LYNCH IN
SUPPORT OF DEFENDANT'S
MOTION FOR ATTORNEYS' FEES

16 I, J. Christopher Lynch, declare as follows:

17 1. I am over 18 years of age and am competent to testify. I make this
18 declaration based on my own personal knowledge. I am one of the attorneys for
19 Defendant, Ryan Lamberson.

SUPPLEMENTAL REPLY DECLARATION OF
J. CHRISTOPHER LYNCH IN
SUPPORT OF DEFENDANT'S MOTION FOR
ATTORNEYS' FEES - 1

LEE & HAYES, PLLC
601 West Riverside Avenue, Suite 1400
Spokane, Washington 99201
Telephone: (509)324-9256 Fax: (509)323-8979

1 2. As I have previously testified, ECF No. 68 at ¶ 25, the timesheets
2 submitted as Exhibit A to ECF No. 100 were prepared from the contemporaneously
3 logged time by each timekeeper whom I assigned to the case. Each timekeeper kept
4 daily time for the matter, identifying all significant tasks and the time spent.

5 3. Tasks subordinate to a significant task were generally not logged as
6 they are presumed within the significant task. The narrative was provided to annotate
7 the main timesheets so that the nature of the tasks taken and the associated time is
8 clear and accurate.

9 4. As I have previously testified, ECF No. 68 at ¶ 25, Mr. Lamberson was
10 sent invoices monthly for payment. Under the Lee & Hayes time and billing system,
11 as the lead counsel on the matter, I was responsible for the “pre-bill” issued during
12 the first week of each month for the previous month’s timekeeper and cost entries
13 for the matter. Each month, I then edited the time and descriptions on the pre-bill to
14 arrive at a fair “final bill” for Mr. Lamberson which was sent to him for payment. I
15 was careful to edit-down time to arrive at a fair amount to charge Mr. Lamberson,
16 an innocent individual with no prior experience as a defendant, who had been
17 dragged into the federal court because of plaintiff’s handlers’ failure to conduct the
18 basic investigation that would have revealed his innocence. Over 30 percent of the
19 time logged to the matter was “written down” in this process; this time (and rate

1 differential) lost was considered an investment by my law firm in our contribution
2 to the cause of fighting copyright abuse in the Eastern District of Washington (ED
3 WA). I assigned tasks to my associates Messrs. Smith and Barney in order to reduce
4 the expense. I edited-out meetings of the three of us or with our staff and interns to
5 arrive at strategy; I retained joint entries where the meeting was a direct report to me
6 as part of an assigned task or the few meetings all of the defense counsel had with
7 Mr. Lamberson because we each had separate areas of work responsibility and
8 reporting responsibilities to him. Although Lee & Hayes has a policy of logging and
9 billing commercial clients for paralegal and intern time, I sought approval from my
10 law firm's management to not charge paralegal and intern time to Mr. Lamberson's
11 account (although the time was logged so that the paralegals and interns could show
12 the firm management their work in connection with Mr. Lamberson's defense).
13 These edited pre-bills became the final bill that is a numbered Lee & Hayes
14 "invoice."

15 5. I "held" the October 2013 time without billing it and then billed it
16 combined with the November 2013 time. Otherwise, I prepared a final bill in the
17 above-stated manner for each month, and the corresponding invoice was sent to Mr.
18 Lamberson for payment. The October 2013 time was held and billed with the
19 November time because I was hopeful that plaintiff would take advantage of the no-

1 money walk-away we had offered, and, in that case, my law firm had agreed not to
2 charge Mr. Lamberson for our time if we could so quickly exonerate him. But as I
3 have testified, the walk-away offer expired without plaintiff examining Mr.
4 Lamberson or his computer or dismissing the case against him. Plaintiff was
5 forewarned that this bad decision came with an obligation to pay attorneys' fees. My
6 law firm had agreed to charge Mr. Lamberson significantly reduced rates due to the
7 horrible spot in which he found himself, as an entirely innocent individual in a mass-
8 defendant federal copyright matter. This was not an ordinary federal civil matter
9 where there may be some question of liability and intellectual property expertise
10 might find a legal path to exoneration – in this case, there was an absolute mistake:
11 Mr. Lamberson had never heard of the movie *Elf-Man* and has no connection to the
12 plaintiff at all. Plaintiff's mistake has had significant personal consequences to each
13 of the innocent defendants like Mr. Lamberson. Plaintiff continues to defend its
14 grave mistakes as somehow societally acceptable, and plaintiff has never
15 acknowledged the mistake nor apologized to Mr. Lamberson. Innocent ISP
16 subscribers need incentive to stop this unlawful extortion racket, not to succumb to
17 it. In over 25 years of intellectual property litigation, I have never represented "more
18 innocent" defendants than these BitTorrent ISP subscribers who had absolutely no
19 connection to the plaintiff that recklessly sued them. The defense attorneys' fee

1 system exists to incentivize innocent individuals not to submit to extortion and to
2 work toward exoneration.

3 6. In the end, Lee & Hayes prepared these monthly bills to Mr. Lamberson
4 for payment: Invoice No. 119919, dated November 30, 2013; Invoice No. 121287,
5 dated December 31, 2013; Invoice No. 123383, dated January 31, 2014; Invoice No.
6 124886, dated February 28, 2014; Invoice No. 126445, dated March 31, 2014;
7 Invoice No. 128101, dated April 30, 2014; Invoice No. 129657, dated May 31, 2014;
8 Invoice No. 131430, dated June 30, 2014; Invoice No. 132939, dated July 31, 2014;
9 Invoice No. 134801, dated August 31, 2014; Invoice No. 136437, dated
10 September 30, 2014; Invoice No. 138355, dated October 31, 2014 and Invoice No.
11 139565 dated November 30, 2014. Each of these invoices is the result of the pre-bill
12 scrub described above and the timesheets submitted here for reimbursement track
13 the time from those invoices and do not in any way submit more time than the
14 invoice billed Mr. Lamberson for payment.

15 7. The timesheets submitted to support this fee request were prepared by
16 me and my staff after the Court ruled in Mr. Lamberson's favor. I had my staff create
17 one document by compiling all of the entries verbatim from each of the Lee & Hayes
18 invoices. Only time that was included on the invoices (i.e. post pre-bill scrub) is
19 included in the timesheets of the request. In other words, the hours requested for this

1 award were all billed to Mr. Lamberson for payment; no hours have been added to
2 the request. Although most of the entries on the submitted timesheets are verbatim
3 from the invoices, as I testified, I did edit some of the entries from the invoices for
4 clarity and detail as to the tasks undertaken, and I did consult the court docket and
5 my attorney correspondence files to do so. Also, attorney-client privilege references
6 were removed. As I have described, the timesheets were scrubbed in good faith to
7 only present those tasks we deemed appropriate to bill to an individual. The
8 timesheets are accurate. The time was logged daily and entered into Lee & Hayes’
9 time and billing system. The hours logged were the subject of monthly bills sent to
10 Mr. Lamberson for payment.

11 8. As I have testified, Mr. Lamberson’s Counterclaims were well founded.
12 Plaintiff asserts it has “immunity” to file baseless lawsuits as part of its extortion
13 scam, but it is overwhelmingly clear that the “sham litigation” exception applies to
14 the claimed immunity. For example, Elf-Man LLC does not deny using fraudulent
15 declarations of a fictitious declarant (“Darren M. Griffin”). Plaintiff does not deny
16 that Crystal Bay Corporation (CBC), the South Dakota company the fictitious
17 declarant (and Mr. Macek) claimed to work for, is not a legally operating entity.
18 Plaintiff does not deny the authenticity of the APMC Prezi presentation I discovered
19 that appears to be the playbook for the use of such deceitful declarations to trick

1 federal judges into granting Subpoenas to obtain subscriber names so that unlawful
2 extortionate demands can be made. This is sham litigation and, thus, the ill effects
3 of it can be the basis for civil liability and equitable relief to deny enforceability of
4 the abused copyright. So, Mr. Lamberson had a right to file counterclaims for money
5 and for equitable relief, but these money counterclaims were withdrawn, as I have
6 testified in ECF No. 100, as a convenience to reduce expense, given plaintiff's
7 transparent attack on the counterclaims and the waste of resources that would have
8 to be undertaken to keep them viable. The money-damages Counterclaims were not
9 withdrawn because they lacked merit, they were withdrawn because plaintiff was
10 frustratingly evasive and deceitful, continually lying about the nature of its lawsuit.
11 I decided to concentrate our resources not on money-damage Counterclaims, but in
12 otherwise enlightening plaintiff's counsel about each of its handlers' fraudulent acts
13 as our investigation uncovered them, hoping that counsel would at some point see
14 the light and do the right thing. Although it has taken over a year, this strategy
15 worked.

16 9. The sanctions motions were well founded: (i) obviously, plaintiff
17 conducted no good faith investigation of Mr. Lamberson before naming him; and
18 (ii) obviously, plaintiff's handlers needlessly multiplied the proceedings being
19 consistently (even predictably) evasive and deceitful about essentially every aspect

1 of the case. The Court had discretion not to award sanctions, but this does not
2 diminish that plaintiff, its counsel, and its handlers engaged in sanctionable conduct
3 throughout the matter.

4 10. Plaintiff's foreign, unidentified handlers are responsible for a tidal
5 wave of fraud on the federal court system. For example, Exhibit D of ECF 95 is a
6 listing of some of the hundreds of cases in which plaintiff's handlers used the
7 declaration of a fake person ("Darren M. Griffin") working for a fake company
8 (Crystal Bay Corporation) submitted to trick federal judges into authorizing
9 Subpoenas so that subscribers could be extorted. Attached hereto as Exhibit A are
10 true and correct copies of the fraudulent declarations of this fake witness working
11 for this fake company filed by Elf-Man LLC and The Thompsons Film LLC.
12 Plaintiff and its counsel do not deny that these fraudulent declarations were filed by
13 Elf-Man LLC; indeed, plaintiff's opposition to the fees, ECF No. 101-1, Exhibit A,
14 shows plaintiff's continued refusal to explain the existence of the fake witness and
15 the fake company it has used in this and other districts. The uses of these fraudulent
16 declarations are unclean hands of the dirtiest variety, presumably amounting to
17 criminal behavior. Plaintiff Elf-Man LLC and its related plaintiffs such as The
18 Thompsons Film LLC should receive no equity from this or any federal court.

1 11. I consulted with other counsel representing innocent defendants sued
2 by plaintiff and its handlers. This was productive and efficient in more quickly
3 uncovering the fraud than my team would have been able to otherwise achieve,
4 especially given plaintiff's evasion and deceit regarding discovery. I did meet with
5 Mr. Matesky about his motion and I did attend Mr. Matesky's FRCP 12(b)(6)
6 Motion in the WD WA as I was working from the Lee & Hayes Seattle office that
7 week. That attendance was productive as I witnessed Ms. VanderMay attempting to
8 explain plaintiff's theories of liability in a manner that she declined to do in
9 correspondence with me. I also witnessed Judge Lasnik challenge Ms. VanderMay's
10 obligations under FRCP 11, where Judge Lasnik offered his opinion that Rule 11
11 could not be complied with as to any of the "subscriber-only" defendants under the
12 facts at hand. Ms. VanderMay later honored this admonition as to the WD WA
13 defendants (by not renaming them after dismissal with leave to amend), but she
14 ignored the admonition as to the ED WA defendants, some of whom are now the
15 subject of default judgments, or still mired in the case that plaintiff has no hope of
16 winning.

17 12. Plaintiff continued to file fraudulent declarations in connection with its
18 opposition to attorneys' fees in this case and in the Motions for Default Judgment in
19 the main cases. For example, as I have testified, plaintiff's handlers stopped using

1 declarations of fake witness “Darren M. Griffin” in mid-November 2013 (after hard
2 questioning in October 2013 about Mr. “Griffin” not only by me, but by a federal
3 judge in Louisiana) – now, the plaintiff’s handlers’ pretend their witness is Daniel
4 Macek, who may in fact be a real person, albeit a person who cannot be deposed
5 without intervention from the State Department and for whom a bogus foreign
6 address has been provided and never corrected. Mr. Macek submitted a declaration
7 in this case, ECF No. 88, claiming to work for Crystal Bay Corporation of South
8 Dakota in its technical department. I have previously testified that CBC does not
9 have a technical department or any legitimate operations and is in no position to hire
10 German nationals to work for it. Just this week, we became informed of Declarations
11 (or their Australian equivalent) of Mr. Macek were submitted to Australian courts
12 where Mr. Macek apparently testified that his investigations were undertaken for
13 “MaverickEye UG” of Germany. Exhibits B, C, and D attached hereto are true and
14 correct copies of articles explaining this. The Australian Court apparently is
15 suspicious of Mr. Macek’s declarations and has ordered him to personally appear in
16 Australia to testify under oath. The plaintiff in the Australian case is Dallas Buyers
17 Club LLC. Dallas Buyers Club LLC is a client of Mr. Lowe’s who has filed several
18 new BitTorrent cases in the WD WA using declarations of Mr. Macek where Mr.
19 Macek claims to have conducted his *Dallas Buyers Club* investigation for Crystal

1 Bay Corporation. As I have testified, these BitTorrent “investigations” are
2 undertaken globally and then sifted by nation and judicial district based on the
3 geolocation of the entrapped IP addresses. So I inquired of Mr. Lowe to explain
4 how Mr. Macek could testify to the WD WA that he conducted his investigation for
5 Crystal Bay Corporation of South Dakota using Crystal Bay Corporation software,
6 but then testify to that Australian court that he somehow simultaneously conducted
7 that identical work for MaverickEye of Germany using MaverickEye software. This
8 is the same logic I used in demanding a plausible explanation about Mr. Macek’s
9 declaration in this case: if the *Elf-Man* investigations are globally performed and
10 then geolocated and sifted into districts, how could “Darren M. Griffin” be the Elf-
11 Man LLC witness in other districts (where no Initial Disclosures were ever
12 provided), but the ED WA witness is somehow Daniel Macek (because Initial
13 Disclosures had been triggered?) Mr. Lowe’s own Exhibit A to ECF 101-1 shows
14 his refusal to explain CBC and its fake witness “Darren M. Griffin.” Our own
15 investigation this past week into MaverickEye showed its ties to IPP, the purported
16 company plaintiff’s handlers’ use as witnesses in pornography cases that may be an
17 alternate name for GuardaLey. (Recall that plaintiff submitted the declaration of
18 Patrick Paige, ECF No. 90, who testified about a test he conducted using IPP
19 software, but without ever explaining how that test of IPP software related to the

1 software Mr. Patzer, in ECF No. 89, said he had designed and assigned to Excipio
2 and that somehow was used by Mr. Macek while somehow working for CBC. The
3 answer to this relation appears to me to be that IPP software does exist, and the
4 remainder of the testimony about Excipio and CBC is testimony fabricated for
5 submission to this Court.) Here are some of the connections I found of MaverickEye
6 to the IPP/Guardaley/CBC criminal guild: (i) MaverickEye has a website,
7 <http://www.maverickeye.de> but the website has no phone number or email method
8 of contact; (ii) the MaverickEye website includes verbatim categories from the
9 website for IPP International, <http://www.ippint.de>; (iii) the MaverickEye website
10 has verbatim language from some of those IPP website categories; (iv) the URL
11 contact for maverickeye.de is an address at ippint.de (just as the APMC URL contact
12 is an address at guardaley.com); (v) the MaverickEye website lists a street address
13 in Stuttgart, Germany that is the same short-term office rental and mailbox address
14 which was the bogus (and never corrected) address we were given for Mr. Macek.
15 So it is no surprise that Mr. Lowe refuses to explain (i) how Mr. Macek testified in
16 the WD WA to have worked for CBC while testifying to somehow simultaneously
17 work for MaverickEye to the Australian court; or (ii) how Mr. Macek testified in the
18 ED WA to have worked for CBC somehow doing the same work simultaneously as
19 a fake person testified that “he” did for that same fake company. Plaintiff and its

1 handlers have defrauded the federal court system (and beyond those borders) and its
2 lawyers are pretending at great lengths that this somehow did not happen.
3 Outrageous!

4 13. We did examine the Declarations of Messrs. Paige, Uebersax, Patzer
5 and Macek and their exhibits as submitted by the plaintiff to support its Motions for
6 Default Judgments in the main case. This was productive since it confirmed there is
7 no additional evidence that plaintiff's handlers have against any of the defendants
8 who were sued. For example, Mr. Patzer never testifies that the investigation of any
9 of the defendants includes actual evidence that the IP address downloaded anything.
10 This confirmed that Mr. Lamberson's case was not unique – the plaintiff has no
11 evidence that *any* defendant downloaded anything, only that an IP address sent a
12 humanly imperceptible packet of data to a foreign investigator's computer at the
13 investigator's request. This is not copyright infringement. Also, we examined the
14 typed-up charts of alleged "additional infringement" of works (that plaintiff does not
15 own and) which would, of course, not be admissible as liability evidence under the
16 FRE (no foundation, plus evidence of prior alleged bad acts are inadmissible.) Recall
17 that we attacked this typed-up chart submitted by Ms. VanderMay, ECF No. 84,
18 Exhibit C, as utterly ridiculous. The chart includes thousands of works allegedly
19 copied over a one-month period, in twelve different languages, at download rates

1 exceeding residential bandwidth, and there is no foundational testimony as to how
2 the typed-up chart was prepared or even that the IP address was assigned to the same
3 subscriber during the entire period the chart purports to cover. So, we examined the
4 typed-up charts later submitted with the default judgments in the main case, ECF
5 No. 128-1. We were not surprised that the charts are in different typographical
6 formats from the one purporting to cover Mr. Lamberson that we had attacked. These
7 new typed-up charts appear to have been re-done to remove ridiculous entries like
8 works in Baku or Mandarin (although a few of the ridiculous foreign works must
9 have been missed including works in Dutch and there is no evidence any of the
10 defaulting defendants speaks Dutch. Also, during the main matter, Ms. VanderMay
11 had mistakenly sent one of these charts that was for another IP address in WD WA,
12 claiming it was for Mr. Lamberson's purported IP address. She later discovered her
13 error and sent us the substitute chart for Mr. Lamberson's purported IP address. She
14 asked us to return the original chart, which we did, but we did note that the original
15 chart, like Mr. Lamberson's was a ridiculous list of works of multiple genres in
16 multiple languages that no ordinary Washington citizen speaks). In other words, it
17 is my conclusion that plaintiff's handlers altered the shotgun data of their original
18 ridiculous typed-up charts to make them seem more plausible as to the defaulting
19 defendants after we had attacked the 12-language chart submitted about Mr.

1 Lamberson. I asked my paralegal to investigate to see if my conclusion was
2 supportable. One of the tasks was to examine publicly-available information about
3 the defaulting defendants and compare it to the charts. The conclusion turned out to
4 be correct – for example, one of the defaulting defendants, Joan Urena, *Thompsons*
5 *Film v. Does 1–35*, 13-cv-00126-TOR (E.D. Wa. 2013) appears only to speak
6 Spanish, but the allegedly infringed works are in English. I concluded that plaintiff’s
7 handlers’ altered the typed-up charts to remove the foreign language titles that
8 somehow end up on these ridiculous shotgun charts, but did so without consideration
9 to what language the defendant spoke. It was not a surprise that the handlers would
10 again fabricate evidence to trick the Court into granting the relief they wanted. We
11 did not perform this investigation to “secure further legal work” as plaintiff’s
12 opposition surmises – we did the work to further confirm that plaintiff and its
13 handlers are engaged in wide-scale fraud on the federal courts. This examination
14 proved fruitful.

15 14. Plaintiff does not dispute that Mr. Lamberson’s offers to resolve the
16 case for no-money were not presented to Elf-Man LLC.

17 15. Mr. Lowe cavalierly claims APMC, Mr. Achache, “Mr. Griffin,” and
18 their crew are unrelated to this matter, but this is not true. Mr. Achache signed the
19 APMC agreement with Vision Films about *Elf-Man*. Mr. Achache has previously

1 testified he works for GuardaLey in the older BitTorrent cases (Ca. 2010-2011.) I
2 was contacted this Tuesday by a lawyer in Dusseldorf, Germany facing a BitTorrent
3 case in Germany; I was informed that Mr. Achache is the witness in that case and he
4 is still claiming to work for GuardaLey to the German court (not IPP or APMC or
5 CBC or MaverickEye). GuardaLey is apparently also known as IPP and may be the
6 real party in interest in this matter. IPP is used as the handler's investigator for
7 pornography cases and the handlers use CBC (or, apparently, MaverickEye or
8 GuardaLey) for the non-pornography cases. CBC is a bogus company and fake "Mr.
9 Griffin" claimed to work for it, just as Mr. Macek does in this case, although Mr.
10 Macek has claimed to the Australian court to perform this work for MaverickEye.
11 All of this filth is connected.

12 16. It is no surprise plaintiff's opposition, ECF 101 at p. 11, includes the
13 wishful thinking that there is "absolutely no identifiable basis relevant to this case
14 for defendant's subpoena to Vision Films." The subpoena to Vision Films was
15 helpful because it confirmed that Vision Films had taken an assignment of many
16 copyright rights from its clients and pursued litigation in its own name, as it had
17 done in the ED TN with *Elf-Man*. The Vision Films subpoena also confirmed the
18 contractual similarities regarding the "coincidence" of *Elf-Man* being loaded into
19 BitTorrent three weeks before its public release date just as had Vision Films' work

1 *Blood Money*. These Vision Films subpoenas helped confirm plaintiff's unlawful
2 scam.

3 17. Plaintiff incorrectly asserts that Mr. Lamberson stipulated to Elf-Man
4 LLC's unilateral cancellation of its own noted deposition. I never agreed to this, and
5 would never have since the alleged conversation occurred before Mr. Lowe was even
6 of record. Plaintiff sought no Protective Order to unilaterally cancel its own noted
7 deposition. Plaintiff's failure to appear at its own noted deposition is additional
8 evidence of its handler's program of sham litigation.

9 18. I am confident that the plaintiff used a falsified Certificate of Service
10 to pretend it had timely provided objections to the APMC discovery. None of the
11 evidence supports the Certificate of Service as being true.

12 19. Part of plaintiff's handlers' scam is to join all defendants in each district
13 in one case, claiming each participated in concert with the others. Plaintiff thus
14 avoided \$11,200 of filing fees in the ED WA and \$60,000 in the WD WA. In fact,
15 however, the percentage chance that plaintiff's joinder allegations are true is zero.
16 Attached as Exhibit E is the declaration of Delvan Neville filed in the Southern
17 District of Indiana wherein he analyzed a ten-defendant BitTorrent case brought by
18 plaintiff's handlers where he examines the plaintiff's joinder allegations and
19 concludes they are a scientific impossibility – in other words, bunk. Legitimate

1 plaintiffs are not allowed to avoid required federal court filing fees, so, *a fortiori*,
2 fraudulent plaintiffs should not be able to avoid them.

3 20. Plaintiff's handlers violated Washington law by using private
4 investigators not licensed or bonded as Washington law requires. Plaintiff's counsel
5 was deceitful about the location of these investigators who are apparently located in
6 Germany (or the United Kingdom or The Netherlands or South Dakota or
7 Sacramento, as the trail of the handlers' lies has proffered). Telephonic depositions
8 of German nationals in a U.S. civil case are unlawful in Germany, and plaintiff
9 provides no contrary evidence. So, of course Mr. Lamberson researched how to
10 lawfully depose these foreign "witnesses."

11 21. As predicted, plaintiff objected to the fee request with the paradoxical
12 argument that Mr. Lamberson should somehow have been able more quickly shed
13 the bogus lawsuit against him. Plaintiff's token offer that Mr. Lamberson is entitled
14 to fewer than 20 hours of fees is bad faith given plaintiff's litany of evasion and
15 deceit. Justice has required Mr. Lamberson to fully brief the fee request since
16 plaintiff has declined to negotiate in good faith.

17 22. Plaintiff's Motion to Dismiss its own case made no provision for
18 compensating Mr. Lamberson, so Mr. Lamberson asked that the dismissal be
19 conditioned upon such payment. Since the law allowed plaintiff to withdraw its

1 motion to dismiss if it found any conditions unacceptable, Mr. Lamberson properly
2 continued briefing of the pending matters. Mr. Lamberson also continued
3 investigation into the lies and fraud plaintiff and its handlers perpetrated on United
4 States District Courts – these lies and fraud are directly relevant to the propriety of
5 a fee award and multiplier as Mr. Lamberson requests.

6 23. Plaintiff again makes the incorrect assertion that its motion to dismiss
7 its own case was prior to Mr. Lamberson's Motion to Compel the APMC discovery.
8 The ECF numbers show that it was not.

9 24. Mr. Lamberson brought a Motion to Strike plaintiff's late-filed
10 response to the Motion to Compel the APMC discovery. If plaintiff's late-filed
11 response had honestly admitted that the Certificate of Service was erroneous, then I
12 would not have moved to strike the pleadings. Instead, the late-filed response took
13 the position that the deceitful Certificate of Service was proper, so I moved to strike
14 the pleadings for being as late, as well as wrong.

15 25. The requested rates are reasonable and significantly under the AIPLA
16 statistics for the experience-level of the three defense counsel. Intellectual property
17 skill was necessary to the defense and hastened resolution of the case – for example,
18 other defendants have answered that they had never heard of *Elf-Man*, but they
19 remain ensnared in the litigation over 20 months since its filing date.

1 26. Unless immediate payment is ordered, it is virtually certain that plaintiff
2 and its handlers will evade payment of the judgment and be deceitful in its collection,
3 just as they have been evasive and deceitful in litigation of the substantive matter. I
4 could supplement the foundation for my conclusion if the Court wishes, but I believe
5 my prior testimony is sufficient to warrant this prediction.

6 27. In over 25 years of intellectual property litigation, I have never
7 encountered the wholesale disregard for the facts, the law, the honor of the Court, or
8 the obligations of counsel to abide by the Federal Rules of Civil Procedure as this
9 case and its related cases have displayed. Ms. VanderMay admitted that “plaintiff’s
10 representatives” were trying to force her into unlawful positions, yet Mr. Lowe
11 perpetuates the pattern of evasion and deceit without ever acknowledging that there
12 might be a problem. Plaintiff’s handlers have devised a scheme to abuse the federal
13 courts as a necessary part of an unlawful extortion campaign. These unidentified
14 handlers collect extorted monies from innocent people every day, but, when their
15 scheme is revealed, they retreat, leaving only the unfortunate copyright holder and
16 its counsel before the Court to face the consequences. I respectfully request that this
17 Court award the full amount requested, doubled under equity, for immediate
18 payment and that the matter be referred to the United States Attorney for
19

1 investigation of the use of fraudulent declarations by Elf-Man LLC in connection
2 with an unlawful extortion scheme.

3 DATED this 12th day of December, 2014.

4 LEE & HAYES, PLLC

5
6 By: J. Christopher Lynch

J. Christopher Lynch, WSBA #17462

Jeffrey R. Smith, WSBA #37460

7 Rhett V. Barney, WSBA #44764

601 W. Riverside Avenue, Suite 1400

8 Spokane, WA 99201

Phone: (509) 324-9256

9 Fax: (509) 323-8979

Emails: chris@leehayes.com

10 jeffreys@leehayes.com

11 rhettb@leehayes.com

12 *Counsel for Defendant Ryan Lamberson*

CERTIFICATE OF SERVICE

I hereby certify that on the 12th day of December, 2014, I caused to be electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the following:

David A. Lowe lowe@lowegrahamjones.com

Collette C. Leland ccl@winstoncashatt.com

LEE & HAYES, PLLC

By: s/ J. Christopher Lynch

J. Christopher Lynch, WSBA #17462
601 W. Riverside Avenue, Suite 1400
Spokane, WA 99201
Phone: (509) 324-9256
Fax: (509) 323-8979
Email: chris@leehayes.com

EXHIBIT A

SUPPLEMENTAL REPLY DECLARATION OF
J. CHRISTOPHER LYNCH IN
SUPPORT OF DEFENDANT'S MOTION FOR
ATTORNEYS' FEES - 23

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. _____

THE THOMPSONS FILM, LLC
a California Limited Liability Company,

Plaintiff,

v.

JOHN DOES 1-94,

Defendants.

DECLARATION OF DARREN M. GRIFFIN IN SUPPORT OF PLAINTIFF'S MOTION
FOR LEAVE TO TAKE LIMITED EXPEDITED DISCOVERY PRIOR TO RULE 26(f)
CONFERENCE

1. My name is Darren M Griffin. I am over the age of 18 and am otherwise competent to make this declaration. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

2. I have been retained as a software consultant by Crystal Bay Corporation CBC ("CBC"), a company incorporated in South Dakota and organized and existing under the laws of the United States, in its technical department. CBC is in the business of providing forensic investigation services to copyright owners.

3. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows hundreds of millions of people around the world to freely and easily exchange ideas and information, including academic research, literary

Exhibit A

works, financial data, music, audiovisual works, graphics, and an unending and ever-changing array of other data.

4. Unfortunately, the Internet also has afforded opportunities for the wide-scale infringement of copyrighted motion pictures.

5. Once a motion picture has been transformed into an unsecured digital format, it can be copied further and distributed an unlimited number of times over the Internet, without significant degradation in picture or sound quality.

6. To copy and distribute copyrighted motion pictures over the Internet, many individuals use online media distribution systems or so-called P2P networks. P2P networks, at least in their most common form, are computer systems that enable Internet users to (1) make files (including motion pictures) stored on each user's computer available for copying by other users; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the Internet.

7. At any given moment and depending on the particular P2P network involved, anywhere from thousands to millions of people, either across the country or around the world, unlawfully use the P2P network to connect to one another's computers to upload (distribute) or download (copy) copyrighted material.

8. The P2P systems represent a "viral" distribution of digital files: each user of the system who copies a digital file from another user can then distribute the file to still other users and so on, so that copies of an infringing file can be distributed to millions of people worldwide with breathtaking speed.

9. Further, a person who uses a P2P network is free to use any alias (or "network

name”) whatsoever, without revealing his or her true identity to other users. Thus, while Plaintiff has observed the infringement occurring on the Internet, it does not know the true identities of those individuals who are committing the infringement.

10. Additionally, the P2P methodologies for which Crystal Bay Corporation monitored for Plaintiff’s Motion Picture make even small computers with low bandwidth capable of participating in large data transfers across a P2P network. The initial file-provider intentionally elects to share a file using a P2P network. This is called “seeding.” Other users (“peers”) on the network connect to the seeder to download. As additional peers request the same file, each additional user becomes a part of the network (or “swarm”) from where the file can be downloaded. However, unlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user who has already downloaded that piece of data, all of which pieces together comprise the whole.

11. This means that every “node” or peer user who has a copy of the infringing copyrighted material on a P2P network—or even a portion of a copy—can also be a source of download for that infringing file, potentially both copying and distributing the infringing work. This distributed nature of P2P leads to a rapid viral spreading of a file throughout peer users. As more peers join the swarm, the likelihood of a successful download increases. Because of the nature of a P2P protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a possible source for the subsequent peer so long as that first seed peer is online at the time the subsequent peer downloads a file.

12. All infringers connected to those files are investigated through downloading a part of the file placed on their computer.

14. Once Crystal Bay Corporation's searching software program identifies an
 er in the way described herein for the Motion Picture for which Plaintiff owns the
 ive licensing and distribution rights, Crystal Bay Corporation obtains the IP address of a
 ffering the file for download.

16. An IP address is a unique numerical identifier that is automatically assigned to an internet user by the user's Internet Service Provider ("ISP"). It only enables Crystal Bay Corporation to trace the infringer's access to the Internet to a particular ISP. Subscribing to and setting up an account with an ISP is the most common and legitimate way for someone to gain access to the Internet. An ISP can be a telecommunications service provider such as Verizon, an Internet service provider such as America Online, a cable Internet service provider such as Comcast, or even an entity such as a university that is large enough to establish its own network and link directly to the Internet.

18. Only the ISP to whom a particular IP address has been assigned for use by its

subscribers can correlate that IP address to a particular subscriber. From time to time, a subscriber of internet services may be assigned different IP addresses from their ISP. Thus, to correlate a subscriber with an IP address, the ISP also needs to know when the IP address was being used. Unfortunately, many ISPs only retain for a very limited amount of time the information necessary to correlate an IP address to a particular subscriber.

19. When available, Crystal Bay Corporation also obtains the user's pseudonym or network name and examines the user's publicly available directory on his or her computer for other files that lexically match Plaintiff's Motion Picture. In addition to the file of the motion picture itself, Crystal Bay Corporation downloads or otherwise collects publicly available information about the network user that is designed to help Plaintiff identify the infringer.

20. The exact manner in which Crystal Bay Corporation determines a user's IP address varies by P2P network.

21. Crystal Bay Corporation determined that the Doe Defendants here were using ISPs listed in Exhibit B to Plaintiff's Motion for Leave to Take Limited Expedited Discovery Prior to Rule 26(f) Conference, together with various other ISPs operating both within and outside the District of Colorado, to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted motion picture.

22. Once Crystal Bay Corporation identified the ISP used by the Doe Defendants to gain access to the Internet from the IP address, an e-mail was sent to the relevant contact at each ISP informing them of the Doe Defendant's IP address and the date and time of the infringing activity.

23. It is possible for digital files to be mislabeled or corrupted; therefore, Crystal Bay

Corporation (and accordingly, Plaintiff) does not rely solely on the labels and metadata attached to the files themselves to determine which motion picture is copied in the downloaded file, but also to confirm through a visual comparison between the downloaded file and the Motion Picture themselves.

24. As to Plaintiff's copyrighted Motion Picture, as identified in the Complaint, a member of Crystal Bay Corporation watches a DVD copy of the Motion Picture provided by Plaintiff.

25. After Crystal Bay Corporation identified the Doe Defendants and downloaded the motion pictures they were distributing, Crystal Bay Corporation opened the downloaded files, watched them and confirmed that they contain a substantial portion of the motion picture identified in the Complaint.

26. Plaintiff retained CBC to identify the IP addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted audiovisual work (the "Work") as identified in Exhibit B of the Complaint. CBC tasked me with analyzing, reviewing and attesting to the results of the investigation.

27. During the performance of my duties as detailed below, I used forensic software provided by CBC to scan peer-to-peer networks for the presence of infringing transactions.

28. After reviewing the evidence logs, I isolated the transactions and the IP addresses of the users responsible for copying and distributing the Work.

29. Through each of the transactions, the computers using the IP addresses identified in Exhibit B attached hereto transmitted a copy or a part of a copy of a digital media file identified by the hash value set forth in Exhibit B attached of Plaintiff's Motion for Leave. The

IP addresses, hash values, dates and times contained in Exhibit B correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Exhibit B were all part of a “swarm” of users that were reproducing, distributing, displaying or performing the copyrighted work identified in Exhibit B.

30. Moreover, the users were sharing the exact same copy of the Work. Any digital copy of an audiovisual work may be uniquely identified by a unique, coded, string of characters called a “hash checksum.” The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as US Secure Hash Algorithm 1 or “SHA-1”, which was developed by the National Security Agency and published as a US government standard. Using a hash tag to identify different copies of the Work, I confirmed that these users reproduced the very same copy of the Work.

31. The CBC software analyzed each BitTorrent “piece” distributed by each IP address listed in Exhibit B and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital motion picture.

32. The software uses a geolocation functionality to confirm that all IP addresses of the users set forth in Exhibit B were located in Colorado. Though an IP address alone does not reveal the name or contact information of the account holder, it does reveal the locations of the Internet line used for the transaction. IP addresses are distributed to ISPs by public, nonprofit organizations called Regional Internet Registries. These registries assign blocks of IP addresses to ISPs by geographic region. In the United States, these blocks are assigned and tracked by the American Registry of Internet Numbers. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly-available and searchable format. An

IP address' geographic location can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial database by ISPs.

33. I have confirmed not only that the users distributed the files in Colorado, but also the specific location where the distribution took place.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 06 day of Nov., 2013.

By: 
Darren M. Griffin

50498770.1

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. _____

ELF-MAN, LLC
a Maryland Limited Liability Company,

Plaintiff,

v.

JOHN DOES 1-85,

Defendants.

**DECLARATION OF DARREN M. GRIFFIN IN SUPPORT OF PLAINTIFF'S MOTION
FOR LEAVE TO TAKE LIMITED EXPEDITED DISCOVERY PRIOR TO RULE 26(f)
CONFERENCE**

1. My name is Darren M Griffin. I am over the age of 18 and am otherwise competent to make this declaration. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

2. I have been retained as a software consultant by Crystal Bay Corporation CBC ("CBC"), a company incorporated in South Dakota and organized and existing under the laws of the United States, in its technical department. CBC is in the business of providing forensic investigation services to copyright owners.

3. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows hundreds of millions of people around the world to freely and easily exchange ideas and information, including academic research, literary

Exhibit A

works, financial data, music, audiovisual works, graphics, and an unending and ever-changing array of other data.

4. Unfortunately, the Internet also has afforded opportunities for the wide-scale infringement of copyrighted motion pictures.

5. Once a motion picture has been transformed into an unsecured digital format, it can be copied further and distributed an unlimited number of times over the Internet, without significant degradation in picture or sound quality.

6. To copy and distribute copyrighted motion pictures over the Internet, many individuals use online media distribution systems or so-called P2P networks. P2P networks, at least in their most common form, are computer systems that enable Internet users to (1) make files (including motion pictures) stored on each user's computer available for copying by other users; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the Internet.

7. At any given moment and depending on the particular P2P network involved, anywhere from thousands to millions of people, either across the country or around the world, unlawfully use the P2P network to connect to one another's computers to upload (distribute) or download (copy) copyrighted material.

8. The P2P systems represent a "viral" distribution of digital files: each user of the system who copies a digital file from another user can then distribute the file to still other users and so on, so that copies of an infringing file can be distributed to millions of people worldwide with breathtaking speed.

9. Further, a person who uses a P2P network is free to use any alias (or "network

name”) whatsoever, without revealing his or her true identity to other users. Thus, while Plaintiff has observed the infringement occurring on the Internet, it does not know the true identities of those individuals who are committing the infringement.

10. Additionally, the P2P methodologies for which Crystal Bay Corporation monitored for Plaintiff’s Motion Picture make even small computers with low bandwidth capable of participating in large data transfers across a P2P network. The initial file-provider intentionally elects to share a file using a P2P network. This is called “seeding.” Other users (“peers”) on the network connect to the seeder to download. As additional peers request the same file, each additional user becomes a part of the network (or “swarm”) from where the file can be downloaded. However, unlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user who has already downloaded that piece of data, all of which pieces together comprise the whole.

11. This means that every “node” or peer user who has a copy of the infringing copyrighted material on a P2P network—or even a portion of a copy—can also be a source of download for that infringing file, potentially both copying and distributing the infringing work. This distributed nature of P2P leads to a rapid viral spreading of a file throughout peer users. As more peers join the swarm, the likelihood of a successful download increases. Because of the nature of a P2P protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a possible source for the subsequent peer so long as that first seed peer is online at the time the subsequent peer downloads a file.

12. All infringers connected to those files are investigated through downloading a part of the file placed on their computer.

13. This evidence is then saved on Crystal Bay Corporation's service.

14. Once Crystal Bay Corporation's searching software program identifies an infringer in the way described herein for the Motion Picture for which Plaintiff owns the exclusive licensing and distribution rights, Crystal Bay Corporation obtains the IP address of a user offering the file for download.

15. The forensic software used by CBC routinely collects, identifies and records the Internet Protocol ("IP") addresses in use by those people who employ the BitTorrent protocol to share, copy, reproduce and distribute copyrighted works.

16. An IP address is a unique numerical identifier that is automatically assigned to an internet user by the user's Internet Service Provider ("ISP"). It only enables Crystal Bay Corporation to trace the infringer's access to the Internet to a particular ISP. Subscribing to and setting up an account with an ISP is the most common and legitimate way for someone to gain access to the Internet. An ISP can be a telecommunications service provider such as Verizon, an Internet service provider such as America Online, a cable Internet service provider such as Comcast, or even an entity such as a university that is large enough to establish its own network and link directly to the Internet.

17. In logs kept in the ordinary course of business, ISPs keep track of the IP addresses assigned to their subscribers. Once provided with an IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and Media Access Control number of the user/subscriber.

18. Only the ISP to whom a particular IP address has been assigned for use by its

subscribers can correlate that IP address to a particular subscriber. From time to time, a subscriber of internet services may be assigned different IP addresses from their ISP. Thus, to correlate a subscriber with an IP address, the ISP also needs to know when the IP address was being used. Unfortunately, many ISPs only retain for a very limited amount of time the information necessary to correlate an IP address to a particular subscriber.

19. When available, Crystal Bay Corporation also obtains the user's pseudonym or network name and examines the user's publicly available directory on his or her computer for other files that lexically match Plaintiff's Motion Picture. In addition to the file of the motion picture itself, Crystal Bay Corporation downloads or otherwise collects publicly available information about the network user that is designed to help Plaintiff identify the infringer.

20. The exact manner in which Crystal Bay Corporation determines a user's IP address varies by P2P network.

21. Crystal Bay Corporation determined that the Doe Defendants here were using ISPs listed in Exhibit B to Plaintiff's Motion for Leave to Take Limited Expedited Discovery Prior to Rule 26(f) Conference, together with various other ISPs operating both within and outside the District of Colorado, to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted motion picture.

22. Once Crystal Bay Corporation identified the ISP used by the Doe Defendants to gain access to the Internet from the IP address, an e-mail was sent to the relevant contact at each ISP informing them of the Doe Defendant's IP address and the date and time of the infringing activity.

23. It is possible for digital files to be mislabeled or corrupted; therefore, Crystal Bay

Corporation (and accordingly, Plaintiff) does not rely solely on the labels and metadata attached to the files themselves to determine which motion picture is copied in the downloaded file, but also to confirm through a visual comparison between the downloaded file and the Motion Picture themselves.

24. As to Plaintiff's copyrighted Motion Picture, as identified in the Complaint, a member of Crystal Bay Corporation watches a DVD copy of the Motion Picture provided by Plaintiff.

25. After Crystal Bay Corporation identified the Due Defendants and downloaded the motion pictures they were distributing, Crystal Bay Corporation opened the downloaded files, watched them and confirmed that they contain a substantial portion of the motion picture identified in the Complaint.

26. Plaintiff retained CBC to identify the IP addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted audiovisual work (the "Work") as identified in Exhibit B of the Complaint. CBC tasked me with analyzing, reviewing and attesting to the results of the investigation.

27. During the performance of my duties as detailed below, I used forensic software provided by CBC to scan peer-to-peer networks for the presence of infringing transactions.

28. After reviewing the evidence logs, I isolated the transactions and the IP addresses of the users responsible for copying and distributing the Work.

29. Through each of the transactions, the computers using the IP addresses identified in Exhibit B attached hereto transmitted a copy or a part of a copy of a digital media file identified by the hash value set forth in Exhibit B attached of Plaintiff's Motion for Leave. The

IP addresses, hash values, dates and times contained in Exhibit B correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Exhibit B were all part of a “swarm” of users that were reproducing, distributing, displaying or performing the copyrighted work identified in Exhibit B.

30. Moreover, the users were sharing the exact same copy of the Work. Any digital copy of an audiovisual work may be uniquely identified by a unique, coded, string of characters called a “hash checksum.” The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as US Secure Hash Algorithm 1 or “SHA-1”, which was developed by the National Security Agency and published as a US government standard. Using a hash tag to identify different copies of the Work, I confirmed that these users reproduced the very same copy of the Work.

31. The CBC software analyzed each BitTorrent “piece” distributed by each IP address listed in Exhibit B and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital motion picture.

32. The software uses a geolocation functionality to confirm that all IP addresses of the users set forth in Exhibit B were located in Colorado. Though an IP address alone does not reveal the name or contact information of the account holder, it does reveal the locations of the Internet line used for the transaction. IP addresses are distributed to ISPs by public, nonprofit organizations called Regional Internet Registries. These registries assign blocks of IP addresses to ISPs by geographic region. In the United States, these blocks are assigned and tracked by the American Registry of Internet Numbers. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly-available and searchable format. An

IP address' geographic location can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial database by ISPs.

33. I have confirmed not only that the users distributed the files in Colorado, but also the specific location where the distribution took place.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 06 day of May, 2013.

By: 
Darren M. Griffin

0098770.1

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI**

Elf-Man, LLC,)	
)	Case No.:
Plaintiff,)	
)	
v.)	
)	
DOES 1-17,)	
)	
Defendants.)	

**DECLARATION OF DARREN M. GRIFFIN IN SUPPORT OF
PLAINTIFF'S MOTION FOR LEAVE TO TAKE DISCOVERY
PRIOR TO RULE 26(f) CONFERENCE**

1. My name is Darren Griffin. I am over the age of 18 and am otherwise competent to make this declaration. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

2. I have been retained as a software consultant by Crystal Bay Corporation ("CBC"), a company incorporated in South Dakota and organized and existing under the laws of the United States, in its technical department. CBC is in the business of providing forensic investigation services to copyright owners.

3. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows hundreds of millions of people around the world to freely and easily exchange ideas and information, including academic research, literary works, financial data, music, audiovisual works, graphics, and an unending and ever-changing array of other data.

4. Unfortunately, the Internet also has afforded opportunities for the wide-scale infringement of copyrighted motion pictures.

5. Once a motion picture has been transformed into an unsecured digital format, it can be copied further and distributed an unlimited number of times over the Internet, without significant degradation in picture or sound quality.

6. To copy and distribute copyrighted motion pictures over the Internet, many individuals use online media distribution systems or so-called P2P networks. P2P networks, at least in their most common form, are computer systems that enable Internet users to (1) make files (including motion pictures) stored on each user's computer available for copying by other users; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the Internet.

7. At any given moment and depending on the particular P2P network involved, anywhere from thousands to millions of people, either across the country or around the world, unlawfully use the P2P network to connect to one another's computers to upload (distribute) or download (copy) copyrighted material.

8. The P2P systems represent a "viral" distribution of digital files: each user of the system who copies a digital file from another user can then distribute the file to still other users and so on, so that copies of an infringing file can be distributed to millions of people worldwide with breathtaking speed.

9. Further, a person who uses a P2P network is free to use any alias (or "network name") whatsoever, without revealing his or her true identity to other users. Thus, while Plaintiff has observed the infringement occurring on the Internet, it does not know the true identities of those individuals who are committing the infringement.

10. Additionally, the P2P methodologies for which Crystal Bay Corporation monitored for Plaintiff's Motion Picture make even small computers with low bandwidth capable of participating in large data transfers across a P2P network. The initial file-provider intentionally

elects to share a file using a P2P network. This is called “seeding.” Other users (“peers”) on the network connect to the seeder to download. As additional peers request the same file, each additional user becomes a part of the network (or “swarm”) from where the file can be downloaded. However, unlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user who has already downloaded that piece of data, all of which pieces together comprise the whole.

11. This means that every “node” or peer user who has a copy of the infringing copyrighted material on a P2P network—or even a portion of a copy—can also be a source of download for that infringing file, potentially both copying and distributing the infringing work simultaneously. This distributed nature of P2P leads to a rapid viral spreading of a file throughout peer users. As more peers join the swarm, the likelihood of a successful download increases. Because of the nature of a P2P protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a possible source for the subsequent peer so long as that first seed peer is online at the time the subsequent peer downloads a file.

12. All infringers connected to those files are investigated through downloading a part of the file placed on their computer.

13. This evidence is then saved on Crystal Bay Corporation’s service.

14. Once Crystal Bay Corporation’s searching software program identifies an infringer in the way described herein for the Motion Picture for which Plaintiff owns the exclusive licensing and distribution rights, Crystal Bay Corporation obtains the IP address of a user offering the file for download.

15. The forensic software used by CBC routinely collects, identifies and records the Internet Protocol (“IP”) addresses in use by those people who employ the BitTorrent protocol to share, copy, reproduce and distribute copyrighted works.

16. An IP address is a unique numerical identifier that is automatically assigned to an internet user by the user's Internet Service Provider ("ISP"). It only enables Crystal Bay Corporation to trace the infringer's access to the Internet to a particular ISP. Subscribing to and setting up an account with an ISP is the most common and legitimate way for someone to gain access to the Internet. An ISP can be a telecommunications service provider such as Verizon, an Internet service provider such as America Online, a cable Internet service provider such as Comcast, or even an entity such as a university that is large enough to establish its own network and link directly to the Internet.

17. In logs kept in the ordinary course of business, ISPs keep track of the IP addresses assigned to their subscribers. Once provided with an IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and Media Access Control number of the user/subscriber.

18. Only the ISP to whom a particular IP address has been assigned for use by its subscribers can correlate that IP address to a particular subscriber. From time to time, a subscriber of internet services may be assigned different IP addresses from their ISP. Thus, to correlate a subscriber with an IP address, the ISP also needs to know when the IP address was being used. Unfortunately, many ISPs only retain for a very limited amount of time the information necessary to correlate an IP address to a particular subscriber.

19. When available, Crystal Bay Corporation also obtains the user's pseudonym or network name and examines the user's publicly available directory on his or her computer for other files that lexically match Plaintiff's Motion Picture. In addition to the file of the motion picture itself, Crystal Bay Corporation downloads or otherwise collects publicly available information about the network user that is designed to help Plaintiff identify the infringer.

20. The exact manner in which Crystal Bay Corporation determines a user's IP address varies by P2P network.

21. Crystal Bay Corporation determined that the Doe Defendants here were using ISPs listed in Exhibit B to Plaintiff's Motion for Leave to Take Discovery Prior to Rule 26(f) Conference, together with various other ISPs operating both within and outside the Eastern District of Missouri, to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted motion picture.

22. It is possible for digital files to be mislabeled or corrupted; therefore, Crystal Bay Corporation (and accordingly, Plaintiff) does not rely solely on the labels and metadata attached to the files themselves to determine which motion picture is copied in the downloaded file, but also to confirm through a visual comparison between the downloaded file and the Motion Picture themselves.

23. As to Plaintiff's copyrighted Motion Picture, as identified in the Complaint, a member of Crystal Bay Corporation watches a DVD copy of the Motion Picture provided by Plaintiff.

24. After Crystal Bay Corporation identified the Doe Defendants and downloaded the motion pictures they were distributing, Crystal Bay Corporation opened the downloaded files, watched them and confirmed that they contain a substantial portion of the motion picture identified in the Complaint.

25. Plaintiff retained CBC to identify the IP addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted audiovisual work as identified in Exhibit A (the "Work"). CBC tasked me with analyzing, reviewing and attesting to the results of the investigation.

26. During the performance of my duties as detailed below, I used forensic software provided by CBC to scan peer-to-peer networks for the presence of infringing transactions.

27. After reviewing the evidence logs, I isolated the transactions and the IP addresses of the users responsible for copying and distributing the Work.

28. Through each of the transactions, the computers using the IP addresses identified in Exhibit B transmitted a copy or a part of a copy of a digital media file identified by the hash value set forth in Exhibit B. The IP addresses, hash values, dates and times contained in Exhibit B correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Exhibit B were all part of a “swarm” of users that were reproducing, distributing, displaying or performing the copyrighted work identified in Exhibit B.

29. Moreover, the users were sharing the exact same copy of the Work. Any digital copy of an audiovisual work may be uniquely identified by a unique, coded, string of characters called a “hash checksum.” The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as US Secure Hash Algorithm 1 or “SHA-1”, which was developed by the National Security Agency and published as a US government standard. Using a hash tag to identify different copies of the Work, I confirmed that these users reproduced the very same copy of the Work.

30. The CBC software analyzed each BitTorrent “piece” distributed by each IP address listed in Exhibit B and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital motion picture.

31. The software uses a geolocation functionality to confirm that all IP addresses of the users set forth in Exhibit B were located in Missouri. Though an IP address alone does not reveal the name or contact information of the account holder, it does reveal the locations of the Internet line used for the transaction. IP addresses are distributed to ISPs by public, nonprofit

organizations called Regional Internet Registries. These registries assign blocks of IP addresses to ISPs by geographic region. In the United States, these blocks are assigned and tracked by the American Registry of Internet Numbers. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly-available and searchable format. An IP address' geographic location can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial database by ISPs.

32. As set forth in Exhibit A, I have confirmed not only that the users distributed the files in Missouri, but also the specific location where the distribution took place.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 27th day of March, 2013.



By: _____
Darren M. Griffin

60998770.1

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

ELF-MAN LLC,)
) Case No.: 13-cv-2362
Plaintiff,)
) Judge Rebecca R. Pallmeyer
v.)
) Magistrate Judge Jeffrey T. Gilbert
DOES 1-82,)
)
Defendants.)

**DECLARATION OF DARREN M. GRIFFIN IN SUPPORT OF
PLAINTIFF'S MOTION FOR LEAVE TO TAKE DISCOVERY
PRIOR TO RULE 26(f) CONFERENCE**

1. I, Darren M. Griffin, make this declaration based on my personal knowledge. If called upon to do so, I will testify that the facts stated herein are true and correct.
2. I have been retained by Crystal Bay Corporation ("CBC"), a corporation of South Dakota, as a software consultant in its technical department. CBC provides forensic investigation services to copyright owners.
3. The forensic software used by CBC routinely collects, identifies and records the Internet Protocol ("IP") addresses in use by those individuals who employ the BitTorrent protocol to share, copy, reproduce and distribute copyrighted works.
4. An IP address is a unique numerical identifier that is automatically assigned to an internet subscriber by the subscriber's Internet Service Provider ("ISP"). Using logs kept in the ordinary course of business, ISPs maintain records of the IP addresses assigned to their subscribers. Once provided with an IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and Media Access Control number of a user/subscriber.

13-cv-2362

5. Only the ISP that has assigned a particular IP address for use by a subscriber can correlate that IP address to a specific subscriber. From time to time, a subscriber of internet services may be assigned different IP addresses by their ISP. Thus, to correlate a subscriber to an IP address, the ISP also needs to know when the IP address was used. Unfortunately, many ISPs only retain the information necessary to correlate an IP address to a particular subscriber for a very limited period of time.

6. Plaintiff retained CBC to identify the IP addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted movie as identified in Exhibit A (the "Work"). CBC directed me to review, analyze and attest to the results of the investigation.

7. During the performance of my duties as detailed below, I used forensic software provided by CBC to scan peer-to-peer networks for the presence of infringing transactions.

8. After reviewing the evidence logs, I isolated the transactions and the IP addresses of the users responsible for copying and distributing the Work.

9. Through each of the transactions, the computers using the IP addresses identified in Exhibit A transmitted a copy or a part of a copy of a digital media file identified by the hash value set forth in Exhibit A. The IP addresses, hash values, dates and times contained in Exhibit A correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Exhibit A were all part of a "swarm" of users who were reproducing, distributing, displaying or performing the copyrighted work identified in Exhibit A.

10. Moreover, the users were sharing the identical copy of the Work. A digital copy of an audiovisual work can be uniquely identified by a unique, coded, string of characters called a "hash checksum." The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as U.S. Secure Hash Algorithm 1 or "SHA-1", which was developed by the National Security Agency and published as a U.S. government standard. Using

13-cv-2362

the hash tag identified in Exhibit A, I confirmed that the users identified as Doe Defendants in Exhibit B to the complaint reproduced and distributed the same copy of the Work.

11. The CBC software analyzed each BitTorrent "piece" distributed by each IP address listed in Exhibit A and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital motion picture.

12. The software uses a geolocation functionality to confirm that all IP addresses of the users set forth in Exhibit A were located in Illinois and, based on information and belief, those users were specifically located in the Northern District of Illinois. Although an IP address alone does not reveal the name or contact information of the subscriber, it does reveal the location of the Internet line used for the transaction. IP addresses are distributed to ISPs by public, nonprofit organizations called Regional Internet Registries. These Registries assign blocks of IP addresses to ISPs by geographic region. In the United States, these blocks are assigned and tracked by the American Registry of Internet Numbers. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly available and searchable format. The geographic location of an IP address can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial databases by ISPs.

13. As set forth in Exhibit A, I have confirmed not only that the users distributed the files in Illinois, but also the specific location (city/town) where the distribution took place.

14. The targeted dates of the swarm in this matter cover a three-month period from early December, 2012 to late February, 2013.

15. Torrent swarms can survive over extended periods of time (months or years) and provide users with exactly the same file comprising exactly the same pieces. The term "piece" is a term of art identifying a portion of a particular file. Based on information and belief, torrent swarms for popular files have been known to be available for over 6 years. The initial seeder (of a

13-cv-2362

parent file) uploads the content and then promotes the torrent file through online forums or websites. Users then have access to the torrent file over the same forums or websites and can join a link to the torrent swarm. Users receive the pieces of the initial seeder and provide those pieces to other users. The transfer occurs piece-by-piece so that the initial pieces from the seeder get passed from one user to the next user.

16. There is no requirement to join an active swarm at a specific date and time. However, a torrent swarm might become smaller after months or years which slows down the process of file sharing activity but still renders the file fully available. A primary factor determining the size of a swarm is the popularity of the product that the file contains (movie, audio, TV series, etc.). For example, a recently released movie can lose popularity within weeks or months, whereas a famous album of a rock band might continue to be popular for several years.

17. In terms of a common nexus of transactions and occurrences, the actions of an individual who downloaded a movie in early December 2012 are connected to the actions of an individual who downloaded the same movie (the same file) as part of the same swarm during early February 2013 in at least the following ways:

- a. A file with a particular hash value downloaded by an individual over that time period can ultimately be traced to a single parent file (i.e., the actions relate back to the same initial seed of the swarm);
- b. The swarm expands over that time period to include additional individuals based on uploading and downloading of pieces of the same file with the same hash value (i.e., the infringement by each individual further advances the series of infringements that began with the initial seed and continued through the actions of other infringers such that all individuals act under the same system); and

13-cv-2362

c. An individual operating a computer with BitTorrent software left "on" over that time period remains a participant of a swarm with respect to any file marked for participation in that swarm (i.e., each individual shares pieces that originated from the same (identical) file, and opens their computer to allow others to connect and receive those pieces).

FURTHER DECLARANT SAYETH NOT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed on this 05th day of April, 2013.

By: 
Darren M. Griffin

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

THE THOMPSONS FILM, LLC,)	
)	Case No.: 13-cv-2368
Plaintiff,)	
)	Judge Joan B. Gottschall
v.)	
)	Magistrate Judge Geraldine Soat Brown
DOES 1-60,)	
)	
Defendants.)	

**DECLARATION OF DARREN M. GRIFFIN IN SUPPORT OF
PLAINTIFF'S MOTION FOR LEAVE TO TAKE DISCOVERY
PRIOR TO RULE 26(f) CONFERENCE**

1. I, Darren M. Griffin, make this declaration based on my personal knowledge. If called upon to do so, I will testify that the facts stated herein are true and correct.
2. I have been retained by Crystal Bay Corporation ("CBC"), a corporation of South Dakota, as a software consultant in its technical department. CBC provides forensic investigation services to copyright owners.
3. The forensic software used by CBC routinely collects, identifies and records the Internet Protocol ("IP") addresses in use by those individuals who employ the BitTorrent protocol to share, copy, reproduce and distribute copyrighted works.
4. An IP address is a unique numerical identifier that is automatically assigned to an internet subscriber by the subscriber's Internet Service Provider ("ISP"). Using logs kept in the ordinary course of business, ISPs maintain records of the IP addresses assigned to their subscribers. Once provided with an IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and Media Access Control number of a user/subscriber.

5. Only the ISP that has assigned a particular IP address for use by a subscriber can correlate that IP address to a specific subscriber. From time to time, a subscriber of internet services may be assigned different IP addresses by their ISP. Thus, to correlate a subscriber to an IP address, the ISP also needs to know when the IP address was used. Unfortunately, many ISPs only retain the information necessary to correlate an IP address to a particular subscriber for a very limited period of time.

6. Plaintiff retained CBC to identify the IP addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted movie as identified in Exhibit A (the "Work"). CBC directed me to review, analyze and attest to the results of the investigation.

7. During the performance of my duties as detailed below, I used forensic software provided by CBC to scan peer-to-peer networks for the presence of infringing transactions.

8. After reviewing the evidence logs, I isolated the transactions and the IP addresses of the users responsible for copying and distributing the Work.

9. Through each of the transactions, the computers using the IP addresses identified in Exhibit A transmitted a copy or a part of a copy of a digital media file identified by the hash value set forth in Exhibit A. The IP addresses, hash values, dates and times contained in Exhibit A correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Exhibit A were all part of a "swarm" of users who were reproducing, distributing, displaying or performing the copyrighted work identified in Exhibit A.

10. Moreover, the users were sharing the identical copy of the Work. A digital copy of an audiovisual work can be uniquely identified by a unique, coded, string of characters called a "hash checksum." The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as U.S. Secure Hash Algorithm 1 or "SHA-1", which was developed by the National Security Agency and published as a U.S. government standard. Using

the hash tag identified in Exhibit A, I confirmed that the users identified as Doe Defendants in Exhibit B to the complaint reproduced and distributed the same copy of the Work.

11. The CBC software analyzed each BitTorrent “piece” distributed by each IP address listed in Exhibit A and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital motion picture.

12. The software uses a geolocation functionality to confirm that all IP addresses of the users set forth in Exhibit A were located in Illinois and, based on information and belief, those users were specifically located in the Northern District of Illinois. Although an IP address alone does not reveal the name or contact information of the subscriber, it does reveal the location of the Internet line used for the transaction. IP addresses are distributed to ISPs by public, nonprofit organizations called Regional Internet Registries. These Registries assign blocks of IP addresses to ISPs by geographic region. In the United States, these blocks are assigned and tracked by the American Registry of Internet Numbers. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly available and searchable format. The geographic location of an IP address can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial databases by ISPs.

13. As set forth in Exhibit A, I have confirmed not only that the users distributed the files in Illinois, but also the specific location (city/town) where the distribution took place.

14. The targeted dates of the swarm in this matter cover a two-month period from early January, 2013 to late February, 2013.

15. Torrent swarms can survive over extended periods of time (months or years) and provide users with exactly the same file comprising exactly the same pieces. The term “piece” is a term of art identifying a portion of a particular file. Based on information and belief, torrent swarms for popular files have been known to be available for over 6 years. The initial seeder (of a

parent file) uploads the content and then promotes the torrent file through online forums or websites. Users then have access to the torrent file over the same forums or websites and can join a link to the torrent swarm. Users receive the pieces of the initial seeder and provide those pieces to other users. The transfer occurs piece-by-piece so that the initial pieces from the seeder get passed from one user to the next user.

16. There is no requirement to join an active swarm at a specific date and time. However, a torrent swarm might become smaller after months or years which slows down the process of file sharing activity but still renders the file fully available. A primary factor determining the size of a swarm is the popularity of the product that the file contains (movie, audio, TV series, etc.). For example, a recently released movie can lose popularity within weeks or months, whereas a famous album of a rock band might continue to be popular for several years.

17. In terms of a common nexus of transactions and occurrences, the actions of an individual who downloaded a movie in early January 2013 are connected to the actions of an individual who downloaded the same movie (the same file) as part of the same swarm during late February 2013 in at least the following ways:

a. A file with a particular hash value downloaded by an individual over that time period can ultimately be traced to a single parent file (i.e., the actions relate back to the same initial seed of the swarm);

b. The swarm expands over that time period to include additional individuals based on uploading and downloading of pieces of the same file with the same hash value (i.e., the infringement by each individual further advances the series of infringements that began with the initial seed and continued through the actions of other infringers such that all individuals act under the same system); and

13-cv-2368

c. An individual operating a computer with BitTorrent software left "on" over that time period remains a participant of a swarm with respect to any file marked for participation in that swarm (i.e., each individual shares pieces that originated from the same (identical) file, and opens their computer to allow others to connect and receive those pieces).

FURTHER DECLARANT SAYETH NOT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed on this 04 day of April, 2013.

By: _____


Darren M. Griffin

infringement of copyrighted motion pictures.

5. Once a motion picture has been transformed into an unsecured digital format, it can be copied further and distributed an unlimited number of times over the Internet, without significant degradation in picture or sound quality.

6. To copy and distribute copyrighted motion pictures over the Internet, many individuals use online media distribution systems or so-called P2P networks. P2P networks, at least in their most common form, are computer systems that enable Internet users to (1) make files (including motion pictures) stored on each user's computer available for copying by other users; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the Internet.

7. At any given moment and depending on the particular P2P network involved, anywhere from thousands to millions of people, either across the country or around the world, unlawfully use the P2P network to connect to one another's computers to upload (distribute) or download (copy) copyrighted material.

8. The P2P systems represent a "viral" distribution of digital files: each user of the system who copies a digital file from another user can then distribute the file to still other users and so on, so that copies of an infringing file can be distributed to millions of people worldwide with breathtaking speed.

9. Further, a person who uses a P2P network is free to use any alias (or "network name") whatsoever, without revealing his or her true identity to other users. Thus, while Plaintiff has observed the infringement occurring on the Internet, it does not know the true identities of those individuals who are committing the infringement.

10. Additionally, the P2P methodologies for which Crystal Bay Corporation monitored for Plaintiff's Motion Picture make even small computers with low bandwidth capable of

participating in large data transfers across a P2P network. The initial file-provider intentionally elects to share a file using a P2P network. This is called “seeding.” Other users (“peers”) on the network connect to the seeder to download. As additional peers request the same file, each additional user becomes a part of the network (or “swarm”) from where the file can be downloaded. However, unlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user who has already downloaded that piece of data, all of which pieces together comprise the whole.

11. This means that every “node” or peer user who has a copy of the infringing copyrighted material on a P2P network—or even a portion of a copy—can also be a source of download for that infringing file, potentially both copying and distributing the infringing work. This distributed nature of P2P leads to a rapid viral spreading of a file throughout peer users. As more peers join the swarm, the likelihood of a successful download increases. Because of the nature of a P2P protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a possible source for the subsequent peer so long as that first seed peer is online at the time the subsequent peer downloads a file.

12. All infringers connected to those files are investigated through downloading a part of the file placed on their computer.

13. This evidence is then saved on Crystal Bay Corporation’s service.

14. Once Crystal Bay Corporation’s searching software program identifies an infringer in the way described herein for the Motion Picture for which Plaintiff owns the exclusive licensing and distribution rights, Crystal Bay Corporation obtains the IP address of a user offering the file for download.

15. The forensic software used by CBC routinely collects, identifies and records the Internet Protocol (“IP”) addresses in use by those people who employ the BitTorrent protocol to

share, copy, reproduce and distribute copyrighted works.

16. An IP address is a unique numerical identifier that is automatically assigned to an internet user by the user's Internet Service Provider ("ISP"). It only enables Crystal Bay Corporation to trace the infringer's access to the Internet to a particular ISP. Subscribing to and setting up an account with an ISP is the most common and legitimate way for someone to gain access to the Internet. An ISP can be a telecommunications service provider such as Verizon, an Internet service provider such as America Online, a cable Internet service provider such as Comcast, or even an entity such as a university that is large enough to establish its own network and link directly to the Internet.

17. In logs kept in the ordinary course of business, ISPs keep track of the IP addresses assigned to their subscribers. Once provided with an IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and Media Access Control number of the user/subscriber.

18. Only the ISP to whom a particular IP address has been assigned for use by its subscribers can correlate that IP address to a particular subscriber. From time to time, a subscriber of internet services may be assigned different IP addresses from their ISP. Thus, to correlate a subscriber with an IP address, the ISP also needs to know when the IP address was being used. Unfortunately, many ISPs only retain for a very limited amount of time the information necessary to correlate an IP address to a particular subscriber.

19. When available, Crystal Bay Corporation also obtains the user's pseudonym or network name and examines the user's publicly available directory on his or her computer for other files that lexically match Plaintiff's Motion Picture. In addition to the file of the motion picture itself, Crystal Bay Corporation downloads or otherwise collects publicly available

information about the network user that is designed to help Plaintiff identify the infringer.

20. The exact manner in which Crystal Bay Corporation determines a user's IP address varies by P2P network.

21. Crystal Bay Corporation determined that the Doe Defendants here were using ISPs listed in Exhibit B to Plaintiff's Motion for Leave to Take Discovery Prior to Rule 26(f) Conference, together with various other ISPs operating both within and outside the Southern District of Ohio, to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted motion picture.

22. Once Crystal Bay Corporation identified the ISP used by the Doe Defendants to gain access to the Internet from the IP address, an e-mail was sent to the relevant contact at each ISP informing them of the Doe Defendant's IP address and the date and time of the infringing activity.

23. It is possible for digital files to be mislabeled or corrupted; therefore, Crystal Bay Corporation (and accordingly, Plaintiff) does not rely solely on the labels and metadata attached to the files themselves to determine which motion picture is copied in the downloaded file, but also to confirm through a visual comparison between the downloaded file and the Motion Picture themselves.

24. As to Plaintiff's copyrighted Motion Picture, as identified in the Complaint, a member of Crystal Bay Corporation watches a DVD copy of the Motion Picture provided by Plaintiff.

25. After Crystal Bay Corporation identified the Doe Defendants and downloaded the motion pictures they were distributing, Crystal Bay Corporation opened the downloaded files, watched them and confirmed that they contain a substantial portion of the motion picture identified in the Complaint.

26. Plaintiff retained CBC to identify the IP addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted audiovisual work as identified in Exhibit B (the "Work"). CBC tasked me with analyzing, reviewing and attesting to the results of the investigation.

27. During the performance of my duties as detailed below, I used forensic software provided by CBC to scan peer-to-peer networks for the presence of infringing transactions.

28. After reviewing the evidence logs, I isolated the transactions and the IP addresses of the users responsible for copying and distributing the Work.

29. Through each of the transactions, the computers using the IP addresses identified in Exhibit B transmitted a copy or a part of a copy of a digital media file identified by the hash value set forth in Exhibit B. The IP addresses, hash values, dates and times contained in Exhibit B correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Exhibit B were all part of a "swarm" of users that were reproducing, distributing, displaying or performing the copyrighted work identified in Exhibit B.

30. Moreover, the users were sharing the exact same copy of the Work. Any digital copy of an audiovisual work may be uniquely identified by a unique, coded, string of characters called a "hash checksum." The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as US Secure Hash Algorithm 1 or "SHA-1", which was developed by the National Security Agency and published as a US government standard. Using a hash tag to identify different copies of the Work, I confirmed that these users reproduced the very same copy of the Work.

31. The CBC software analyzed each BitTorrent "piece" distributed by each IP address listed in Exhibit B and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital motion picture.

32. The software uses a geolocation functionality to confirm that all IP addresses of the users set forth in Exhibit B were located in Ohio. Though an IP address alone does not reveal the name or contact information of the account holder, it does reveal the locations of the Internet line used for the transaction. IP addresses are distributed to ISPs by public, nonprofit organizations called Regional Internet Registries. These registries assign blocks of IP addresses to ISPs by geographic region. In the United States, these blocks are assigned and tracked by the American Registry of Internet Numbers. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly-available and searchable format. An IP address' geographic location can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial database by ISPs.

33. As set forth in Exhibit A, I have confirmed not only that the users distributed the files in Ohio, but also the specific location where the distribution took place.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 19 day of April, 2013.

By: 
Darren M Griffin

60998770.1

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

THE THOMPSONS FILM, LLC,

Plaintiff,

CASE NO.:

v.

DOE 3,

Defendant.

_____/

**DECLARATION OF DARREN M. GRIFFIN IN SUPPORT OF THE
THOMPSONS FILM LLC'S, MOTION FOR LEAVE TO SERVE NON-PARTY
SUBPOENA PRIOR TO RULE 26(f) CONFERENCE AND SUPPORTING
MEMORANDUM OF LAW**

I, Darren M. Griffin, declare:

1. I work for Crystal Bay Cooperation CBC, "Crystal Bay", a company incorporated in South Dakota with its principal address at 110E Center Street, Suite 2013, Madison, South Dakota 57042. Crystal Bay is a provider of online anti-piracy services for the motion picture industry. Before my employment with Crystal Bay, I held various positions at companies that developed software technologies. I have approximately ten years of experience related to digital media and computer technology.

2. I submit this declaration in support of Plaintiff's Motion for Leave to Serve Non-Party Subpoenas Prior to Rule 26(f) Conference. This declaration is based on my personal knowledge, and if called upon to do so, I would be prepared to testify as to its truth and accuracy.

EXHIBIT B
Thompsons 4-3

3. At Crystal Bay, I am the head of the department that carries out evidence collection and provides litigation support services. I work closely with our research team to create credible processes to scan for, detect, and download copies of copyrighted material on multiple network protocols for use by copyright owners.

4. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows hundreds of millions of people around the world to freely and easily exchange ideas and information, including academic research, literary works, financial data, music, audiovisual works, graphics, and an unending and ever-changing array of other data. Unfortunately, the Internet also has afforded opportunities for the wide-scale infringement of copyrighted motion pictures. Once a motion picture has been transformed into an unsecured digital format, it can be copied further and distributed an unlimited number of times over the Internet, without significant degradation in picture or sound quality.

5. To copy and distribute copyrighted motion pictures over the Internet, many individuals use online media distribution systems or so-called "peer-to-peer" ("P2P") networks. P2P networks, at least in their most common form, are computer systems that enable Internet users to (1) make files (including motion pictures) stored on each user's computer available for copying by other users or peers; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the Internet.

6. On behalf of Plaintiff, we engaged in a specific process using Crystal Bay's specially designed software technology to identify direct infringers of Plaintiff's

copyrighted materials using protocols investigated by Crystal Bay's software on P2P networks. Crystal Bay has documented evidence of the unauthorized reproduction and distribution of the copyrighted motion picture to which Plaintiff holds the exclusive distribution and licensing rights, *The Thompsons* (the "Motion Picture"), within the United States of America, including the Middle District of Florida.

7. Because the Plaintiff has not authorized its copyrighted Motion Picture to be copied or distributed in unsecured P2P networks, I believe that the copying and distribution of the Motion Picture on P2P networks violates the copyright laws.

8. Crystal Bay has licensed a proprietary technology that provides an effective means to detect the unauthorized distribution of movies and other content and files over online media distribution systems, or P2P networks. Crystal Bay's technology enables it to detect and monitor the unlawful transfer and distribution of files amongst the P2P networks by different protocols. Those protocols make even small computers with low bandwidth capable of participating in large data transfers across a P2P network. The initial file-provider intentionally elects to share a file with P2P networks. This is called "seeding." Other users ("peers") on the network connect to the seed file to download.

9. The particular P2P protocol at issue in this suit is called "BitTorrent." What makes BitTorrent unique is that, as yet additional peers request the same file, each additional user becomes a part of the network from where the file can be downloaded. However, unlike a traditional P2P network, each new file downloader is receiving a portion of the data from each connected user who has already downloaded a part of the file that together comprises the whole. This means that every "node" or user who has a

copy of the infringing copyrighted material on a P2P network investigated by our software must necessarily also be a source of download for that infringing file.

10. Specifically, the BitTorrent process works as follows: Users intentionally download a small program that they install on their computers – the BitTorrent “client” application. The BitTorrent client is the user’s interface during the downloading/uploading process. There are many different BitTorrent clients, all of which are readily available on the Internet for free.

11. BitTorrent client applications typically lack the ability to search for torrent files. To find torrent files available for download (as made available by other BitTorrent users), users intentionally visit torrent sites using any standard web browser

12. A torrent site is a website that contains an index of torrent files being made available by other users (generally an extensive listing of movies and television programs, among other copyrighted content). The torrent site hosts and distributes these small torrent files. Although torrent files do not contain actual audio/visual media, they instruct a user’s computer where to go and how to get the desired file. In essence, the torrent file contains a “roadmap” to the IP addresses of other users who are sharing the media file identified by the unique hash identifier, as well as specifics about the media file. Torrent files interact with specific trackers, allowing the user to download the desired file.

13. The torrent file contains a unique hash identifier, which is a unique identifier generated by a mathematical algorithm developed by the National Security Agency. This torrent file is tagged with the file’s unique “info-hash,” which acts as a

“roadmap” to the addresses of other users who are sharing the media file identified by the unique info-hash, as well as specifics about the media file. The hash identifier of the torrent files utilized by Doe 3 and its peers to illegally distribute and share Plaintiff’s Motion Picture is as follows:

SHA1: B7942734E80EC3726A9CBC08FE9B46BA8BFE7220 (“Hash SHA1: B794”).

14. A BitTorrent tracker manages the distribution of files, connecting uploaders (those who are distributing content) with downloaders (those who are copying the content). A tracker directs a BitTorrent user’s computer to other users who have a particular file, and then facilitates the download process from those users. When a BitTorrent user seeks to download a movie or television file, he or she merely clicks on the appropriate hash file on a torrent site, and the torrent file instructs the client software how to connect to a tracker that will identify where the file is available to begin downloading it. In addition to a tracker, a user can manage file distribution through a Distributed Hash Table. Furthermore, a so-called Peer-Exchange is used to retrieve more users for the specific file.

15. Files downloaded in this method are downloaded in hundreds of individual pieces. Each piece that is downloaded is immediately thereafter made available for distribution to other users seeking the same file. The effect of this technology makes every downloader also an uploader of the content. This means that every user who has a copy of the infringing material on a torrent network must necessarily also be a source of download for that material.

16. In order to have engaged in the unauthorized distribution and sharing of Plaintiff's copyrighted Motion Picture, each of the participating peers intentionally obtained a torrent file for Plaintiff's Motion Picture from the video index of a BitTorrent website or other torrent site. Each of the participating peers then intentionally loaded that torrent file into a computer program downloaded onto their computer that is specifically designed to read such files. With the torrent file loaded, the BitTorrent program employed the BitTorrent protocol to initiate simultaneous connections to hundreds of other peers possessing and sharing copies of the digital media – Plaintiff's Motion Picture – described in the torrent file.

17. Once connected, the program began coordinating the copying of Plaintiff's Motion Picture among participating peer computers. As the film was copied to the peers' computers piece by piece, the downloaded pieces were immediately made available to other connected peers seeking to obtain the file.

18. Each of the peers is a member of a single "swarm" or group of BitTorrent peers whose computers are collectively connected for the sharing of a particular hash file, in this instance, Plaintiff's Motion Picture, and this swarm is associated with is the foregoing unique has identifier.

19. Peer Exchange is a communications protocol built into almost every BitTorrent protocol, which allows swarm members to share files more quickly and efficiently. Peer Exchange is responsible for helping all other swarm members participate in illegal file sharing, regardless of geographical boundaries.

20. A Distributed Hash Table is a sort of world-wide telephone book, which uses each file's "info-hash" (a unique identifier for each torrent file) to locate sources for the requested data. Thus, swarm members are able to access a partial list of swarm members rather than being filtered through a central computer called a tracker. By allowing members of the swarm to rely on individual computers for information, this not only reduces the load on the central tracker, but also means that every client that is sharing this data is also helping to hold this worldwide network together.

21. Each of the peers participated in the swarm for the purpose of the reproduction and distribution of Plaintiff's Motion Picture.

22. The distributed nature of the P2P networks typically leads to a rapid viral spreading of a file throughout peer users. As more peers join the collective swarm, the frequency of successful downloads also increases. Because of the nature of a BitTorrent protocol, any user who has downloaded a file prior to the time that subsequent user downloads the same file is automatically a source for the subsequent peer, so long as that first user is online at the time the subsequent user request the file from the swarm. Because of the nature of the swarm, every infringer is – and by necessity all infringers together are – simultaneously both stealing the Plaintiff's copyrighted material and redistributing it. Millions of people have used P2P networks to distribute copyrighted material.

23. Crystal Bay used the search function of the P2P network to look for network users who were offering for distribution audiovisual files that were labeled with the names of Plaintiff's copyrighted Motion Picture. Crystal Bay then conducted a

download of the respective content and a careful and thorough review of that data. The unique hash identifier of the file was extracted from the original torrent file as soon as the content had been verified as a valid copy of Plaintiff's copyrighted Motion Picture. Crystal Bay started searching for individuals making the content identified by the hash value available to the public. When a network user was located who was making that content available for distribution, Crystal Bay downloaded a part of the that file and stored other specific information in order to confirm that infringement was occurring and to identify the infringer by the unique Internet Protocol ("IP") address assigned to Doe 3 by his/her ISP on the date and at the time of the Doe 3's infringing activity.

24. Doe 3 and its peer infringers in the swarm were identified in the following way: Crystal Bay's software is connected to the *The Thompsons* file, an illegal version of the Motion Picture. All infringers connected to the file will be investigated through downloading a part of the file placed on their computer. This evidence is saved on our server and could be shown to the court as evidence if necessary.

25. Once Crystal Bay's searching software program identifies an infringer in the way described herein for the Motion Picture for which Plaintiff owns the exclusive licensing and distribution rights, we obtain the Internet Protocol ("IP") address of a user offering the file for download. In addition to the file of the Motion Picture itself, we download or otherwise collect publicly available information about the network user that is designed to help Plaintiff identify the infringer. Among other things, we download or record for each file downloaded: (a) the time and date at which the file or a part of the file was distributed by the user; (b) the IP address assigned to each user at the time of

infringement; (c) the ISP for each infringer; and, in some cases, (d) the video file's metadata (digital data about the file), such as title and file size, that is not part of the actual video content, but that is attached to the digital file and helps identify the content of the file, (e) the BitTorrent client application used by each user, (f) the global unique identifier for each file downloaded by each user, and (g) the location of most users (by state) at the time of download as determined by geolocation technology. We then create evidence logs for each user and store all this information in a database.

The Need for Expedited Discovery

26. Obtaining the identity of copyright infringers, including Doe 3, on an expedited basis is critical to prosecution of this action and stopping the continued infringement of this copyrighted Motion Picture. Without expedited discovery in the instant case, Plaintiff has no way of serving Doe 3 with the Complaint and Summons in this case. Plaintiff does not have Doe 3's name, address, e-mail address, telephone number, or any other way to identify or locate Doe 3, other than the unique IP address assigned to Doe 3 by his/her Internet Service Provider on the date and at the time of Doe 3's infringing activity.

27. Further, Internet Service Providers ("ISPs") have different policies pertaining to the length of time they preserve session data which identifies their subscribers. Despite requests to preserve the information, some ISPs keep the session data of their subscribers' activities for only limited periods of time – sometimes as little as weeks or even days – before erasing the data they contain. If an ISP does not have to

respond expeditiously to a discovery request, the identification in that ISP's logs may be erased.

28. An IP address is, in combination with the date, a unique numerical identifier that is automatically assigned to a user by its ISP each time a user logs on to the network. Each time a subscriber logs on, he or she may be assigned a different IP address unless the user obtains from his/her ISP a static IP address. ISPs are assigned certain blocks or ranges of IP addresses. ISPs keep track of the IP addresses assigned to its subscribers at any given moment and retain such "user logs" for a very limited amount of time. These user logs provide the most accurate means to connect an infringer's identity to its infringing activity.

29. Although users' IP addresses are not automatically displayed on the P2P networks, any user's IP address is readily identifiable from the packets of data being exchanged. The exact manner in which we determine a user's IP address varies by P2P network.

30. An infringer's IP address is significant because it becomes a unique identifier that, along with the date and time of infringement, specifically identifies a particular computer using the Internet. However, the IP address does not enable us to ascertain with certainty the exact physical location of the computer or to determine the infringer's identity. It only enables us to trace the infringer's access to the Internet to a particular ISP and, in some instances, to a general geographic area. Subscribing to and setting up an account with an ISP is the most common and legitimate way for someone to gain access to the Internet. An ISP can be a telecommunications service provider such as

Verizon, an Internet service provider such as America Online, a cable Internet service provider such as Comcast, or even an entity such as a university that is large enough to establish its own network and link directly to the Internet.

31. Here, the IP address Crystal Bay identified for Plaintiff enabled us to determine which ISP was used by Doe 3 to gain access to the Internet. Publicly available databases located on the Internet list the IP address ranges assigned to various ISPs. However, some ISPs lease or otherwise allocate certain of their IP addresses to other unrelated, intermediary ISPs. Since these ISPs consequently have no direct relationship – customer, contractual, or otherwise – with the end-user, they are unable to identify the infringers through reference to their user logs. The intermediary ISP's own user logs, however, should permit identification of Doe 3. We determined that Doe 3 was using the ISP listed in Exhibit A to Plaintiff's Motion, to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted Motion Picture.

32. We downloaded the entire copyrighted Motion Picture, and other identifying information described above, reviewed it and added such information to our monitoring system. Subsequently, we created evidence logs for a small part of the motion picture file for Doe 3. Once the ISP is provided with the IP address, plus the date and time of the infringing activity, Doe 3's ISP quickly and easily can use its subscriber logs to identify the name and address of the ISP subscriber who was assigned that IP address at that date and time.

Confirmation of Downloaded Material

33. I am also responsible for identifying on-line piracy of motion pictures for Crystal Bay, including gathering evidence of on-line piracy to support counsel's copyright enforcement efforts.

34. As part of my responsibilities at Crystal Bay, I have been designated to confirm that the digital audiovisual files downloaded by Crystal Bay are actual copies of Plaintiff's Motion Picture. It is possible for digital files to be mislabeled or corrupted; therefore, Crystal Bay (and accordingly, Plaintiff) does not rely solely on the labels and metadata attached to the files themselves to determine which motion picture is copied in the downloaded file, but also to confirm through a visual comparison between the downloaded file and the motion picture itself.

35. As to Plaintiff's copyrighted Motion Picture, as identified in the Complaint, one of my assistants or I have watched a copy of the Motion Picture provided by Plaintiff. The downloaded files have been carefully reviewed and compared by a visual comparison with the original motion picture. We have confirmed that they contain a substantial portion of the Motion Picture identified in the Complaint and that at least the Motion Picture DVD case displays a copyright notice.

36. Plaintiff's Motion Picture continues to be made available for unlawful transfer and distribution using P2P protocols, in violation of Plaintiff's exclusive licensing and distribution rights, and rights in the copyright. Crystal Bay continues to monitor such unlawful distribution and transfer of Plaintiff's Motion Picture and to identify infringers.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on April 24, 2013



Darren M. Griffin

5. Once a motion picture has been transformed into an unsecured digital format, it can be copied further and distributed an unlimited number of times over the Internet, without significant degradation in picture or sound quality.

6. To copy and distribute copyrighted motion pictures over the Internet, many individuals use online media distribution systems or so-called P2P networks. P2P networks, at least in their most common form, are computer systems that enable Internet users to (1) make files (including motion pictures) stored on each user's computer available for copying by other users; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the Internet.

7. At any given moment and depending on the particular P2P network involved, anywhere from thousands to millions of people, either across the country or around the world, unlawfully use the P2P network to connect to one another's computers to upload (distribute) or download (copy) copyrighted material.

8. The P2P systems represent a "viral" distribution of digital files: each user of the system who copies a digital file from another user can then distribute the file to still other users and so on, so that copies of an infringing file can be distributed to millions of people worldwide with breathtaking speed.

9. Further, a person who uses a P2P network is free to use any alias (or "network name") whatsoever, without revealing his or her true identity to other users. Thus, while Plaintiff has observed the infringement occurring on the Internet, it does not know the true identities of those individuals who are committing the infringement.

10. Additionally, the P2P methodologies for which Crystal Bay Corporation monitored for Plaintiff's Motion Picture make even small computers with low bandwidth capable of participating in large data transfers across a P2P network. The initial file-provider intentionally

elects to share a file using a P2P network. This is called “seeding.” Other users (“peers”) on the network connect to the seeder to download. As additional peers request the same file, each additional user becomes a part of the network (or “swarm”) from where the file can be downloaded. However, unlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user who has already downloaded that piece of data, all of which pieces together comprise the whole.

11. This means that every “node” or peer user who has a copy of the infringing copyrighted material on a P2P network—or even a portion of a copy—can also be a source of download for that infringing file, potentially both copying and distributing the infringing work. This distributed nature of P2P leads to a rapid viral spreading of a file throughout peer users. As more peers join the swarm, the likelihood of a successful download increases. Because of the nature of a P2P protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a possible source for the subsequent peer so long as that first seed peer is online at the time the subsequent peer downloads a file.

12. All infringers connected to those files are investigated through downloading a part of the file placed on their computer.

13. This evidence is then saved on Crystal Bay Corporation’s service.

14. Once Crystal Bay Corporation’s searching software program identifies an infringer in the way described herein for the Motion Picture for which Plaintiff owns the exclusive licensing and distribution rights, Crystal Bay Corporation obtains the IP address of a user offering the file for download.

15. The forensic software used by CBC routinely collects, identifies and records the Internet Protocol (“IP”) addresses in use by those people who employ the BitTorrent protocol to share, copy, reproduce and distribute copyrighted works.

16. An IP address is a unique numerical identifier that is automatically assigned to an internet user by the user's Internet Service Provider ("ISP"). It only enables Crystal Bay Corporation to trace the infringer's access to the Internet to a particular ISP. Subscribing to and setting up an account with an ISP is the most common and legitimate way for someone to gain access to the Internet. An ISP can be a telecommunications service provider such as Verizon, an Internet service provider such as America Online, a cable Internet service provider such as Comcast, or even an entity such as a university that is large enough to establish its own network and link directly to the Internet.

17. In logs kept in the ordinary course of business, ISPs keep track of the IP addresses assigned to their subscribers. Once provided with an IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and Media Access Control number of the user/subscriber.

18. Only the ISP to whom a particular IP address has been assigned for use by its subscribers can correlate that IP address to a particular subscriber. From time to time, a subscriber of internet services may be assigned different IP addresses from their ISP. Thus, to correlate a subscriber with an IP address, the ISP also needs to know when the IP address was being used. Unfortunately, many ISPs only retain for a very limited amount of time the information necessary to correlate an IP address to a particular subscriber.

19. When available, Crystal Bay Corporation also obtains the user's pseudonym or network name and examines the user's publicly available directory on his or her computer for other files that lexically match Plaintiff's Motion Picture. In addition to the file of the motion picture itself, Crystal Bay Corporation downloads or otherwise collects publicly available information about the network user that is designed to help Plaintiff identify the infringer.

20. The exact manner in which Crystal Bay Corporation determines a user's IP address varies by P2P network.

21. Crystal Bay Corporation determined that the Doe Defendants here were using ISPs listed in Exhibit B to Plaintiff's Motion for Leave to Take Discovery Prior to Rule 26(f) Conference, together with various other ISPs operating both within and outside the Northern District of Ohio, to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted motion picture.

22. Once Crystal Bay Corporation identified the ISP used by the Doe Defendants to gain access to the Internet from the IP address, an e-mail was sent to the relevant contact at each ISP informing them of the Doe Defendant's IP address and the date and time of the infringing activity.

23. It is possible for digital files to be mislabeled or corrupted; therefore, Crystal Bay Corporation (and accordingly, Plaintiff) does not rely solely on the labels and metadata attached to the files themselves to determine which motion picture is copied in the downloaded file, but also to confirm through a visual comparison between the downloaded file and the Motion Picture themselves.

24. As to Plaintiff's copyrighted Motion Picture, as identified in the Complaint, a member of Crystal Bay Corporation watches a DVD copy of the Motion Picture provided by Plaintiff.

25. After Crystal Bay Corporation identified the Doe Defendants and downloaded the motion pictures they were distributing, Crystal Bay Corporation opened the downloaded files, watched them and confirmed that they contain a substantial portion of the motion picture identified in the Complaint.

26. Plaintiff retained CBC to identify the IP addresses of those BitTorrent users who

were copying and distributing Plaintiff's copyrighted audiovisual work as identified in Exhibit B (the "Work"). CBC tasked me with analyzing, reviewing and attesting to the results of the investigation.

27. During the performance of my duties as detailed below, I used forensic software provided by CBC to scan peer-to-peer networks for the presence of infringing transactions.

28. After reviewing the evidence logs, I isolated the transactions and the IP addresses of the users responsible for copying and distributing the Work.

29. Through each of the transactions, the computers using the IP addresses identified in Exhibit B transmitted a copy or a part of a copy of a digital media file identified by the hash value set forth in Exhibit B. The IP addresses, hash values, dates and times contained in Exhibit B correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Exhibit B were all part of a "swarm" of users that were reproducing, distributing, displaying or performing the copyrighted work identified in Exhibit B.

30. Moreover, the users were sharing the exact same copy of the Work. Any digital copy of an audiovisual work may be uniquely identified by a unique, coded, string of characters called a "hash checksum." The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as US Secure Hash Algorithm 1 or "SHA-1", which was developed by the National Security Agency and published as a US government standard. Using a hash tag to identify different copies of the Work, I confirmed that these users reproduced the very same copy of the Work.

31. The CBC software analyzed each BitTorrent "piece" distributed by each IP address listed in Exhibit B and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital motion picture.

32. The software uses a geolocation functionality to confirm that all IP addresses of

the users set forth in Exhibit B were located in Ohio. Though an IP address alone does not reveal the name or contact information of the account holder, it does reveal the locations of the Internet line used for the transaction. IP addresses are distributed to ISPs by public, nonprofit organizations called Regional Internet Registries. These registries assign blocks of IP addresses to ISPs by geographic region. In the United States, these blocks are assigned and tracked by the American Registry of Internet Numbers. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly-available and searchable format. An IP address' geographic location can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial database by ISPs.

33. As set forth in Exhibit A, I have confirmed not only that the users distributed the files in Ohio, but also the specific location where the distribution took place.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 23 day of April, 2013.

By: 

Darren M Griffin

60998770.1

ELF-MAN, LLC)
)
Plaintiff,) CA. _____
)
v.) Judge _____
)
DOES 1-36)
)
Defendants.)

1. My name is Darren M Griffin. I am over the age of 18 and am otherwise competent to make this declaration. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.
2. I have been retained as a software consultant by Crystal Bay Corporation CBC ("CBC"), a company incorporated in South Dakota and organized and existing under the laws of the United States, in its technical department. CBC is in the business of providing forensic investigation services to copyright owners.
3. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows hundreds of millions of people around the world to freely and easily exchange ideas and information, including academic research, literary works, financial data, music, audiovisual works, graphics, and an unending and ever-changing array of other data.
4. Unfortunately, the Internet also has afforded opportunities for the wide-scale infringement of copyrighted motion pictures.
5. Once a motion picture has been transformed into an unsecured digital format, it can

be copied further and distributed an unlimited number of times over the Internet, without significant degradation in picture or sound quality.

6. To copy and distribute copyrighted motion pictures over the Internet, many individuals use online media distribution systems or so-called P2P networks. P2P networks, at least in their most common form, are computer systems that enable Internet users to (1) make files (including motion pictures) stored on each user's computer available for copying by other users; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the Internet.

7. At any given moment and depending on the particular P2P network involved, anywhere from thousands to millions of people, either across the country or around the world, unlawfully use the P2P network to connect to one another's computers to upload (distribute) or download (copy) copyrighted material.

8. The P2P systems represent a "viral" distribution of digital files: each user of the system who copies a digital file from another user can then distribute the file to still other users and so on, so that copies of an infringing file can be distributed to millions of people worldwide with breathtaking speed.

9. Further, a person who uses a P2P network is free to use any alias (or "network name") whatsoever, without revealing his or her true identity to other users. Thus, while Plaintiff has observed the infringement occurring on the Internet, it does not know the true identities of those individuals who are committing the infringement.

10. Additionally, the P2P methodologies for which Crystal Bay Corporation monitored for Plaintiff's Motion Picture make even small computers with low bandwidth capable of participating in large data transfers across a P2P network. The initial file-provider intentionally elects to share a file using a P2P network. This is called "seeding." Other users ("peers") on the

network connect to the seeder to download. As additional peers request the same file, each additional user becomes a part of the network (or “swarm”) from where the file can be downloaded. However, unlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user who has already downloaded that piece of data, all of which pieces together comprise the whole.

11. This means that every “node” or peer user who has a copy of the infringing copyrighted material on a P2P network—or even a portion of a copy—can also be a source of download for that infringing file, potentially both copying and distributing the infringing work. This distributed nature of P2P leads to a rapid viral spreading of a file throughout peer users. As more peers join the swarm, the likelihood of a successful download increases. Because of the nature of a P2P protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a possible source for the subsequent peer so long as that first seed peer is online at the time the subsequent peer downloads a file.

12. All infringers connected to those files are investigated through downloading a part of the file placed on their computer.

13. This evidence is then saved on Crystal Bay Corporation’s service.

14. Once Crystal Bay Corporation’s searching software program identifies an infringer in the way described herein for the Motion Picture for which Plaintiff owns the exclusive licensing and distribution rights, Crystal Bay Corporation obtains the IP address of a user offering the file for download.

15. The forensic software used by CBC routinely collects, identifies and records the Internet Protocol (“IP”) addresses in use by those people who employ the BitTorrent protocol to share, copy, reproduce and distribute copyrighted works.

16. An IP address is a unique numerical identifier that is automatically assigned to an

internet user by the user's Internet Service Provider ("ISP"). It only enables Crystal Bay Corporation to trace the infringer's access to the Internet to a particular ISP. Subscribing to and setting up an account with an ISP is the most common and legitimate way for someone to gain access to the Internet. An ISP can be a telecommunications service provider such as Verizon, an Internet service provider such as America Online, a cable Internet service provider such as Comcast, or even an entity such as a university that is large enough to establish its own network and link directly to the Internet.

17. In logs kept in the ordinary course of business, ISPs keep track of the IP addresses assigned to their subscribers. Once provided with an IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and Media Access Control number of the user/subscriber.

18. Only the ISP to whom a particular IP address has been assigned for use by its subscribers can correlate that IP address to a particular subscriber. From time to time, a subscriber of internet services may be assigned different IP addresses from their ISP. Thus, to correlate a subscriber with an IP address, the ISP also needs to know when the IP address was being used. Unfortunately, many ISPs only retain for a very limited amount of time the information necessary to correlate an IP address to a particular subscriber.

19. When available, Crystal Bay Corporation also obtains the user's pseudonym or network name and examines the user's publicly available directory on his or her computer for other files that lexically match Plaintiff's Motion Picture. In addition to the file of the motion picture itself, Crystal Bay Corporation downloads or otherwise collects publicly available information about the network user that is designed to help Plaintiff identify the infringer.

20. The exact manner in which Crystal Bay Corporation determines a user's IP address

varies by P2P network.

21. Crystal Bay Corporation determined that the Doe Defendants here were using ISPs listed in Exhibit B to Plaintiff's Motion for Leave to Take Discovery Prior to Rule 26(f) Conference, together with various other ISPs operating both within and outside the Southern District of Ohio, to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted motion picture.

22. Once Crystal Bay Corporation identified the ISP used by the Doe Defendants to gain access to the Internet from the IP address, an e-mail was sent to the relevant contact at each ISP informing them of the Doe Defendant's IP address and the date and time of the infringing activity.

23. It is possible for digital files to be mislabeled or corrupted; therefore, Crystal Bay Corporation (and accordingly, Plaintiff) does not rely solely on the labels and metadata attached to the files themselves to determine which motion picture is copied in the downloaded file, but also to confirm through a visual comparison between the downloaded file and the Motion Picture themselves.

24. As to Plaintiff's copyrighted Motion Picture, as identified in the Complaint, a member of Crystal Bay Corporation watches a DVD copy of the Motion Picture provided by Plaintiff.

25. After Crystal Bay Corporation identified the Doe Defendants and downloaded the motion pictures they were distributing, Crystal Bay Corporation opened the downloaded files, watched them and confirmed that they contain a substantial portion of the motion picture identified in the Complaint.

26. Plaintiff retained CBC to identify the IP addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted audiovisual work as identified in Exhibit B

(the "Work"). CBC tasked me with analyzing, reviewing and attesting to the results of the investigation.

27. During the performance of my duties as detailed below, I used forensic software provided by CBC to scan peer-to-peer networks for the presence of infringing transactions.

28. After reviewing the evidence logs, I isolated the transactions and the IP addresses of the users responsible for copying and distributing the Work.

29. Through each of the transactions, the computers using the IP addresses identified in Exhibit B transmitted a copy or a part of a copy of a digital media file identified by the hash value set forth in Exhibit B. The IP addresses, hash values, dates and times contained in Exhibit B correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Exhibit B were all part of a "swarm" of users that were reproducing, distributing, displaying or performing the copyrighted work identified in Exhibit B.

30. Moreover, the users were sharing the exact same copy of the Work. Any digital copy of an audiovisual work may be uniquely identified by a unique, coded, string of characters called a "hash checksum." The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as US Secure Hash Algorithm 1 or "SHA-1", which was developed by the National Security Agency and published as a US government standard. Using a hash tag to identify different copies of the Work, I confirmed that these users reproduced the very same copy of the Work.

31. The CBC software analyzed each BitTorrent "piece" distributed by each IP address listed in Exhibit B and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital motion picture.

32. The software uses a geolocation functionality to confirm that all IP addresses of the users set forth in Exhibit B were located in Ohio. Though an IP address alone does not reveal

the name or contact information of the account holder, it does reveal the locations of the Internet line used for the transaction. IP addresses are distributed to ISPs by public, nonprofit organizations called Regional Internet Registries. These registries assign blocks of IP addresses to ISPs by geographic region. In the United States, these blocks are assigned and tracked by the American Registry of Internet Numbers. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly-available and searchable format. An IP address' geographic location can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial database by ISPs.

33. As set forth in Exhibit A, I have confirmed not only that the users distributed the files in Ohio, but also the specific location where the distribution took place.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 23 day of April, 2013.

By: _____



Darren M Griffin

60998770.1

ELF-MAN LLC,
Plaintiff,
v.
DOES 1-82,
Defendants.

)
) **Case No.: 13-cv-2362**
)
) **Judge Rebecca R. Pallmeyer**
)
) **Magistrate Judge Jeffrey T. Gilbert**
)
)
)

1. I, Darren M. Griffin, make this declaration based on my personal knowledge. If called upon to do so, I will testify that the facts stated herein are true and correct.
2. I have been retained by Crystal Bay Corporation ("CBC"), a corporation of South Dakota, as a software consultant in its technical department. CBC provides forensic investigation services to copyright owners.
3. The forensic software used by CBC routinely collects, identifies and records the Internet Protocol ("IP") addresses in use by those individuals who employ the BitTorrent protocol to share, copy, reproduce and distribute copyrighted works.
4. An IP address is a unique numerical identifier that is automatically assigned to an internet subscriber by the subscriber's Internet Service Provider ("ISP"). Using logs kept in the ordinary course of business, ISPs maintain records of the IP addresses assigned to their subscribers. Once provided with an IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and Media Access Control number of a user/subscriber.

Case: 1:13-cv-03884 Document #: 9-1 Filed: 07/03/13 Page 3 of 10 PageID #:41

Case: 1:13-cv-02362 Document #: 9-1 Filed: 04/05/13 Page 3 of 28 PageID #:38

13-cv-2362

5. Only the ISP that has assigned a particular IP address for use by a subscriber can correlate that IP address to a specific subscriber. From time to time, a subscriber of internet services may be assigned different IP addresses by their ISP. Thus, to correlate a subscriber to an IP address, the ISP also needs to know when the IP address was used. Unfortunately, many ISPs only retain the information necessary to correlate an IP address to a particular subscriber for a very limited period of time.

6. Plaintiff retained CBC to identify the IP addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted movie as identified in Exhibit A (the "Work"). CBC directed me to review, analyze and attest to the results of the investigation.

7. During the performance of my duties as detailed below, I used forensic software provided by CBC to scan peer-to-peer networks for the presence of infringing transactions.

8. After reviewing the evidence logs, I isolated the transactions and the IP addresses of the users responsible for copying and distributing the Work.

9. Through each of the transactions, the computers using the IP addresses identified in Exhibit A transmitted a copy or a part of a copy of a digital media file identified by the hash value set forth in Exhibit A. The IP addresses, hash values, dates and times contained in Exhibit A correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Exhibit A were all part of a "swarm" of users who were reproducing, distributing, displaying or performing the copyrighted work identified in Exhibit A.

10. Moreover, the users were sharing the identical copy of the Work. A digital copy of an audiovisual work can be uniquely identified by a unique, coded, string of characters called a "hash checksum." The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as U.S. Secure Hash Algorithm 1 or "SHA-1", which was developed by the National Security Agency and published as a U.S. government standard. Using

Case: 1:13-cv-03884 Document #: 9-1 Filed: 07/03/13 Page 4 of 10 PageID #:42

Case: 1:13-cv-02362 Document #: 9-1 Filed: 04/05/13 Page 4 of 28 PageID #:39

13-cv-2362

the hash tag identified in Exhibit A, I confirmed that the users identified as Doe Defendants in Exhibit B to the complaint reproduced and distributed the same copy of the Work.

11. The CBC software analyzed each BitTorrent "piece" distributed by each IP address listed in Exhibit A and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital motion picture.

12. The software uses a geolocation functionality to confirm that all IP addresses of the users set forth in Exhibit A were located in Illinois and, based on information and belief, those users were specifically located in the Northern District of Illinois. Although an IP address alone does not reveal the name or contact information of the subscriber, it does reveal the location of the Internet line used for the transaction. IP addresses are distributed to ISPs by public, nonprofit organizations called Regional Internet Registries. These Registries assign blocks of IP addresses to ISPs by geographic region. In the United States, these blocks are assigned and tracked by the American Registry of Internet Numbers. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly available and searchable format. The geographic location of an IP address can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial databases by ISPs.

13. As set forth in Exhibit A, I have confirmed not only that the users distributed the files in Illinois, but also the specific location (city/town) where the distribution took place.

14. The targeted dates of the swarm in this matter cover a three-month period from early December, 2012 to late February, 2013.

15. Torrent swarms can survive over extended periods of time (months or years) and provide users with exactly the same file comprising exactly the same pieces. The term "piece" is a term of art identifying a portion of a particular file. Based on information and belief, torrent swarms for popular files have been known to be available for over 6 years. The initial seeder (of a

Case: 1:13-cv-03884 Document #: 9-1 Filed: 07/03/13 Page 5 of 10 PageID #:43

Case: 1:13-cv-02362 Document #: 9-1 Filed: 04/05/13 Page 5 of 28 PageID #:40

13-cv-2362

parent file) uploads the content and then promotes the torrent file through online forums or websites. Users then have access to the torrent file over the same forums or websites and can join a link to the torrent swarm. Users receive the pieces of the initial seeder and provide those pieces to other users. The transfer occurs piece-by-piece so that the initial pieces from the seeder get passed from one user to the next user.

16. There is no requirement to join an active swarm at a specific date and time. However, a torrent swarm might become smaller after months or years which slows down the process of file sharing activity but still renders the file fully available. A primary factor determining the size of a swarm is the popularity of the product that the file contains (movie, audio, TV series, etc.). For example, a recently released movie can lose popularity within weeks or months, whereas a famous album of a rock band might continue to be popular for several years.

17. In terms of a common nexus of transactions and occurrences, the actions of an individual who downloaded a movie in early December 2012 are connected to the actions of an individual who downloaded the same movie (the same file) as part of the same swarm during early February 2013 in at least the following ways:

a. A file with a particular hash value downloaded by an individual over that time period can ultimately be traced to a single parent file (i.e., the actions relate back to the same initial seed of the swarm);

b. The swarm expands over that time period to include additional individuals based on uploading and downloading of pieces of the same file with the same hash value (i.e., the infringement by each individual further advances the series of infringements that began with the initial seed and continued through the actions of other infringers such that all individuals act under the same system); and

Case: 1:13-cv-03884 Document #: 9-1 Filed: 07/03/13 Page 6 of 10 PageID #:44

Case: 1:13-cv-02362 Document #: 9-1 Filed: 04/05/13 Page 6 of 28 PageID #:41

13-cv-2362

c. An individual operating a computer with BitTorrent software left "on" over that time period remains a participant of a swarm with respect to any file marked for participation in that swarm (i.e., each individual shares pieces that originated from the same (identical) file, and opens their computer to allow others to connect and receive those pieces).

FURTHER DECLARANT SAYETH NOT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed on this 05th day of April, 2013.

By: 
Darren M. Griffin

Case: 1:13-cv-04293 Document #: 7-1 Filed: 07/09/13 Page 2 of 10 PageID #:40

Case: 1:13-cv-02362 Document #: 9-1 Filed: 04/05/13 Page 2 of 28 PageID #:37

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

ELF-MAN LLC,)	
)	Case No.: 13-cv-2362
Plaintiff,)	
)	Judge Rebecca R. Pallmeyer
v.)	
)	Magistrate Judge Jeffrey T. Gilbert
DOES 1-82,)	
)	
Defendants.)	

**DECLARATION OF DARREN M. GRIFFIN IN SUPPORT OF
PLAINTIFF'S MOTION FOR LEAVE TO TAKE DISCOVERY
PRIOR TO RULE 26(f) CONFERENCE**

1. I, Darren M. Griffin, make this declaration based on my personal knowledge. If called upon to do so, I will testify that the facts stated herein are true and correct.
2. I have been retained by Crystal Bay Corporation ("CBC"), a corporation of South Dakota, as a software consultant in its technical department. CBC provides forensic investigation services to copyright owners.
3. The forensic software used by CBC routinely collects, identifies and records the Internet Protocol ("IP") addresses in use by those individuals who employ the BitTorrent protocol to share, copy, reproduce and distribute copyrighted works.
4. An IP address is a unique numerical identifier that is automatically assigned to an internet subscriber by the subscriber's Internet Service Provider ("ISP"). Using logs kept in the ordinary course of business, ISPs maintain records of the IP addresses assigned to their subscribers. Once provided with an IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and Media Access Control number of a user/subscriber.

Case: 1:13-cv-04293 Document #: 7-1 Filed: 07/09/13 Page 3 of 10 PageID #:41

Case: 1:13-cv-02362 Document #: 9-1 Filed: 04/05/13 Page 3 of 28 PageID #:38

13-cv-2362

5. Only the ISP that has assigned a particular IP address for use by a subscriber can correlate that IP address to a specific subscriber. From time to time, a subscriber of internet services may be assigned different IP addresses by their ISP. Thus, to correlate a subscriber to an IP address, the ISP also needs to know when the IP address was used. Unfortunately, many ISPs only retain the information necessary to correlate an IP address to a particular subscriber for a very limited period of time.

6. Plaintiff retained CBC to identify the IP addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted movie as identified in Exhibit A (the "Work"). CBC directed me to review, analyze and attest to the results of the investigation.

7. During the performance of my duties as detailed below, I used forensic software provided by CBC to scan peer-to-peer networks for the presence of infringing transactions.

8. After reviewing the evidence logs, I isolated the transactions and the IP addresses of the users responsible for copying and distributing the Work.

9. Through each of the transactions, the computers using the IP addresses identified in Exhibit A transmitted a copy or a part of a copy of a digital media file identified by the hash value set forth in Exhibit A. The IP addresses, hash values, dates and times contained in Exhibit A correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Exhibit A were all part of a "swarm" of users who were reproducing, distributing, displaying or performing the copyrighted work identified in Exhibit A.

10. Moreover, the users were sharing the identical copy of the Work. A digital copy of an audiovisual work can be uniquely identified by a unique, coded, string of characters called a "hash checksum." The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as U.S. Secure Hash Algorithm 1 or "SHA-1", which was developed by the National Security Agency and published as a U.S. government standard. Using

Case: 1:13-cv-04293 Document #: 7-1 Filed: 07/09/13 Page 4 of 10 PageID #:42

Case: 1:13-cv-02362 Document #: 9-1 Filed: 04/05/13 Page 4 of 28 PageID #:39

13-cv-2362

the hash tag identified in Exhibit A, I confirmed that the users identified as Doe Defendants in Exhibit B to the complaint reproduced and distributed the same copy of the Work.

11. The CBC software analyzed each BitTorrent "piece" distributed by each IP address listed in Exhibit A and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital motion picture.

12. The software uses a geolocation functionality to confirm that all IP addresses of the users set forth in Exhibit A were located in Illinois and, based on information and belief, those users were specifically located in the Northern District of Illinois. Although an IP address alone does not reveal the name or contact information of the subscriber, it does reveal the location of the Internet line used for the transaction. IP addresses are distributed to ISPs by public, nonprofit organizations called Regional Internet Registries. These Registries assign blocks of IP addresses to ISPs by geographic region. In the United States, these blocks are assigned and tracked by the American Registry of Internet Numbers. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly available and searchable format. The geographic location of an IP address can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial databases by ISPs.

13. As set forth in Exhibit A, I have confirmed not only that the users distributed the files in Illinois, but also the specific location (city/town) where the distribution took place.

14. The targeted dates of the swarm in this matter cover a three-month period from early December, 2012 to late February, 2013.

15. Torrent swarms can survive over extended periods of time (months or years) and provide users with exactly the same file comprising exactly the same pieces. The term "piece" is a term of art identifying a portion of a particular file. Based on information and belief, torrent swarms for popular files have been known to be available for over 6 years. The initial seeder (of a

Case: 1:13-cv-04293 Document #: 7-1 Filed: 07/09/13 Page 5 of 10 PageID #:43

Case: 1:13-cv-02362 Document #: 9-1 Filed: 04/05/13 Page 5 of 28 PageID #:40

13-cv-2362

parent file) uploads the content and then promotes the torrent file through online forums or websites. Users then have access to the torrent file over the same forums or websites and can join a link to the torrent swarm. Users receive the pieces of the initial seeder and provide those pieces to other users. The transfer occurs piece-by-piece so that the initial pieces from the seeder get passed from one user to the next user.

16. There is no requirement to join an active swarm at a specific date and time.

However, a torrent swarm might become smaller after months or years which slows down the process of file sharing activity but still renders the file fully available. A primary factor determining the size of a swarm is the popularity of the product that the file contains (movie, audio, TV series, etc.). For example, a recently released movie can lose popularity within weeks or months, whereas a famous album of a rock band might continue to be popular for several years.

17. In terms of a common nexus of transactions and occurrences, the actions of an individual who downloaded a movie in early December 2012 are connected to the actions of an individual who downloaded the same movie (the same file) as part of the same swarm during early February 2013 in at least the following ways:

a. A file with a particular hash value downloaded by an individual over that time period can ultimately be traced to a single parent file (i.e., the actions relate back to the same initial seed of the swarm);

b. The swarm expands over that time period to include additional individuals based on uploading and downloading of pieces of the same file with the same hash value (i.e., the infringement by each individual further advances the series of infringements that began with the initial seed and continued through the actions of other infringers such that all individuals act under the same system); and

Case: 1:13-cv-04293 Document #: 7-1 Filed: 07/09/13 Page 6 of 10 PageID #:44

Case: 1:13-cv-02362 Document #: 9-1 Filed: 04/05/13 Page 6 of 28 PageID #:41

13-cv-2362

c. An individual operating a computer with BitTorrent software left "on" over that time period remains a participant of a swarm with respect to any file marked for participation in that swarm (i.e., each individual shares pieces that originated from the same (identical) file, and opens their computer to allow others to connect and receive those pieces).

FURTHER DECLARANT SAYETH NOT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed on this 08th day of April, 2013.

By: 
Darren M. Griffin

EXHIBIT B

SUPPLEMENTAL REPLY DECLARATION OF
J. CHRISTOPHER LYNCH IN
SUPPORT OF DEFENDANT'S MOTION FOR
ATTORNEYS' FEES - 101

[About](#) [Contact](#) [Archives](#)

Search...



BREAKING

ISP WANTS TO UNDERSTAND TECHNOLOGY USED TO TRACK PIRATES

BY **ANDY** ON **NOVEMBER 10, 2014**C: **33**

Legal representatives for ISP iiNet say they want an anti-piracy tracking system put under the microscope. Hundreds of the Aussie service providers customers are at risk of being sent "speculative invoices" demanding cash for alleged infringements but iiNet definitely isn't going to give plaintiff Dallas Buyers Club an easy ride.

Following a leak of the movie Dallas Buyers Club onto the Internet in January 2013, owner Voltage Pictures took the opportunity to extract cash payments from hundreds of US citizens said to have downloaded the movie.



The practice is lucrative, so much so that the company is now testing the Australian market. Among others, Dallas Buyers Club LLC (DBCLLC) are targeting subscribers of iiNet, a local ISP with a reputation for defending its customers.

<http://torrentfreak.com/isp-wants-to-understand-technology-used-to-track-pirates-141110/> 12/11/2014

(DBCLLC) recently applied to the Federal Court to have iiNet and others reveal the identities of people they say have downloaded and/or shared their movie without permission, but to date iiNet (which also owns fellow targeted ISPs Internode and Adam) is [opposing the application](#) for discovery.

Earlier today the parties were in Federal Court in Sydney before Justice Nye Perram. DBCLLC wants iiNet to hand over its subscribers' identities, but the ISP suspects that instead of giving targets their day in court the movie company simply wants to scare settlements out of them.

According to [ZDNet](#), Barrister Richard Lancaster, SC representing iiNet, told Justice Perram that the ISP needs to know more about the anti-piracy tracking system that was used to track the alleged copyright infringers.

DBCLLC hired Stuttgart, Germany based outfit MaverickEye UG, an outfit that claims to provide "world-class surveillance" of intellectual property on the leading P2P networks including BitTorrent. The company also claims experience with other law firms operating similar pay-up-or-else business models.

"Maverickeye UG work very closely with several law firms focused on the protection of intellectual property and specialized in filing legal claims against people who infringe on your intellectual property," the company [says](#) on its website.

It's now also becoming clearer why DBCLLC selected iiNet as a target. In its prolonged legal battle with movie company Village Roadshow which concluded two years ago, iiNet said it would've handed over subscriber information had there been a successful application to the High Court. DBCLLC lawyer Ian Pike told the Court today that he will indeed be relying on those statements.

Next Monday will see another hearing, this time on the issue of security and costs. To ensure that it's not left with a huge legal bill, iiNet has requested that DBCLLC deposit AUS\$100,00 (US\$86,700) into a holding account in the event the movie company loses in its bid to obtain the ISP's customers' details. That amount is already in dispute with DBCLLC reportedly prepared to put forward just AUS\$30,000 (US\$26,000).

During December another hearing will determine whether iiNet will be able to call Maverick Eye's Daniel Macek as a witness to determine whether the company's anti-piracy tracking system is up to the job of identifying an infringer.

Then, during February 5 and 6, 2015, the full case will be heard. A win for iiNet could mean a significant setback for DBCLLC, while a victory could signal a green light to other companies plotting similar action. In the United States, DBCLLC demands payment of up to US\$7,000 (AUS\$8,000) from each person it targets.

Tagged in: [Dallas Buyers Club](#), [Maverick Eye](#)

[Previous Post...](#)[Next Post...](#)

Share this post

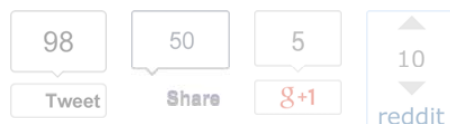



EXHIBIT C


SUPPLEMENTAL REPLY DECLARATION OF
J. CHRISTOPHER LYNCH IN
SUPPORT OF DEFENDANT'S MOTION FOR
ATTORNEYS' FEES - 105

Business News

dailytelegraph.com.au

Business

Subscribe and get **EXTRA EXTRA SPORT** 

Daily Telegraph  [Find out more](#)

STOCK QUOTES

iiNet and Dallas Buyers Club set for February courtroom showdown

- by: Supratim Adhikari
- November 10, 2014 1:45PM

Share

x

Share this story

- Facebook
- Twitter
- LinkedIn
- Google
- Email

Ads By Google

- Top Franchises For 2014**
Franchises Starting Under \$30,000 Compare 100s of low cost franchises
franchisehelp.com/CheapFranchise

The legal fracas between internet service provider iiNet and copyright litigant Dallas Buyers Club LLC is set to kick up a notch with the first hearing of the case in the federal court scheduled for early February.

<http://www.dailytelegraph.com.au/business/breaking-news/iinet-and-dallas-buyers-club-s...> 12/11/2014

While February 5 and 6 have been set as the stipulated days for the hearing, an iiNet spokesperson told Business Spectator that the final dates still need to be negotiated.

Dallas LLC will this Wednesday need to provide iiNet with the information regarding its use of German firm called Maverick Eye, whose technology was purportedly used to track and identify the unique internet protocol (IP) addresses of iiNet customers who were allegedly using BitTorrent to access the movie Dallas Buyers Club.

A directions hearing is also set for December 5, which will determine if iiNet could call one Daniel Macek as a witness to elucidate how Maverick Eye's technology is used to identify copyright infringers and determine the validity of the technology used.

Meanwhile, both iiNet and Dallas LLC are set to lock horns on November 17 in a "security of costs" hearing, with iiNet seeking Dallas LLC to deposit \$100,000 into a third party account to cover iiNet's legal fees in case the copyright litigant loses its bid to obtain personal details of iiNet customers.

An iiNet spokesperson said that Dallas LLC was only keen on a deposit of \$30,000.

The legal imbroglio between iiNet and Dallas LLC officially kicked off in October, when the copyright litigant initiated a 'preliminary discovery' action in a bid to obtain personal details of some iiNet customers who allegedly used BitTorrent to download copyrighted content.

The practice of 'preliminary discovery' is a common precursor to IP litigation but, in order to determine the identity of the defendant.

iiNet has stuck to its guns with regards to withholding the details, saying that they will be used by Dallas LLC to indulge in speculative invoicing, a problem quite common in the United States.

According to Queensland University of Technology's Adjunct Law Professor Dan Hunter, speculative invoicing is far less prevalent in Australia.

"Some copyright trolls have made a habit of seeding movies on BitTorrent, bringing preliminary discovery motions, and then sending out "settlement" agreements for large sums," Professor Hunter said.

"Because the US system has really punitive damages (which we don't have in Australia) the amounts are staggering, and often defendants will pay-especially for pornographic downloads because they don't want the publicity."

"It's unclear whether speculative invoicing is that much of a problem in Australia. You don't hear that much about it," he added.

However, the stoush between iiNet and Dallas LLC could set an interesting precedent, which the ISP says will have an implication on whether customers could be left at the mercy of speculative invoicing.

According to iiNet, Dallas LLC needs to not only spell out what it intends to do with the customers information but also clarify the technology used to track and identify infringers.

- **facebook**
- **twitter**
- **linkedin**

<http://www.dailytelegraph.com.au/business/breaking-news/iinet-and-dallas-buyers-club-s...> 12/11/2014

- **google +**
 - **reddit**
 - **email**
-

EXHIBIT D

SUPPLEMENTAL REPLY DECLARATION OF
J. CHRISTOPHER LYNCH IN
SUPPORT OF DEFENDANT'S MOTION FOR
ATTORNEYS' FEES - 109

JUST IN: *IT buying: Why can't governments ever get it right?*

Topic: *Piracy*

Dallas Buyers Club to pay up for expert witness flight

Summary: *The expert that Dallas Buyers Club LLC used to determine which Australian customers allegedly shared the film online will be flown from Germany to Australia for cross-examination.*



By Josh Taylor | December 2, 2014 -- 00:12 GMT (16:12 PST)

Follow @joshgnosis

15.5K followers

The key witness that Dallas Buyers Club LLC is relying on in order to force iiNet and other internet service providers (ISPs) to hand over the details of customers alleged to have downloaded infringing copies of *Dallas Buyers Club* will be flown from Germany to Australia for cross-examination.

iiNet and several other ISPs including Dodo are fighting an [attempt by Dallas Buyers Club LLC \(/article/iinet-in-new-legal-battle-against-film-studios-over-piracy/\)](#) to obtain customer details for IP addresses that were tracked by the organisation on torrents for the film.

iiNet had been receiving letters from the firm involved in the case [since mid-2013 \(/article/iinet-seeks-info-on-dallas-buyers-club-piracy-investigation/\)](#), [before the release of the *Dallas Buyers Club* film \(http://www.zdnet.com/piracy-warning-letters-sent-to-iinet-before-film-leak-7000035736/\)](#), and it was revealed that the law firm had used a German company, Maverickeye UG. According to [the company's website \(http://www.maverickeye.de/services/\)](#), the organisation uses "highly sophisticated software" and "robust hardware infrastructure" to obtain data that has "quality, consistency, and relevance" for the legal system.

In other jurisdictions where the firm has obtained customer details, so-called speculative invoices have been sent to customers demanding thousands of dollars in compensation, or risk facing court action from the firm.

iiNet is seeking to test the reliability and accuracy of the software, and requested that an expert witness who compiled the still-private expert report come to Australia for cross-examination. iiNet seeks to firstly determine whether the software used to match IP addresses with those of its customers, and the other ISPs' customers, is reliable, and then to ask the expert how it can differentiate between whether an account holder matched to that IP address has infringed, or whether someone else accessing that account, such as a person in a house using the Wi-Fi network, could have instead infringed.

Barrister for Dallas Buyers Club LLC Ian Pike, in a directions hearing in the Federal Court on Tuesday, resisted bringing the witness to Australia from Germany, given the cost involved in flights to Australia.

Pike read out from the expert report that the witness "scans the internet to identify the IP addresses of users that are making digital movies available", and has identified a number of IP addresses associated with the ISPs in Australia.

"[Your point is] who cares how he has done it; he has got the numbers," Justice Nye Perram said.

iiNet barrister Richard Lancaster SC said that he seeks to test the accuracy of the software, and for that, the witness needs to be cross-examined.

"It would not be appropriate for a respective applicant ... threatening account holders in circumstances where the account holder may not be aware of the use of an IP address at a particular time," he said.

He said that Dallas Buyers Club LLC "bringing a witness they rely on" is part and parcel of the discovery process in seeking to obtain the customer details of alleged infringers.

Latest Australian news

[New houses to be charged for NBN fibre \(/article/new-houses-to-be-charged-for-the-nbn-fibre/\)](#)

[Australia's security agencies quiet on metadata definition \(/article/asio-afp-quiet-on-metadata-definition/\)](#)

[ISPs ready to crack down on online piracy with industry code \(/article/isps-ready-to-develop-industry-code-to-crack-down-on-online-piracy/\)](#)

[Stop the torrents: ISPs to block piracy websites, send warnings \(/article/australian-isps-forced-to-block-piracy-websites-send-warnings/\)](#)

[Australia looks to unlock crowdfunding \(/article/australia-looks-to-unlock-crowd-funding/\)](#)

<http://www.zdnet.com/article/dallas-buyers-club-to-pay-up-for-expert-witness-flight/>

12/11/2014

SUPPLEMENTAL REPLY DECLARATION OF
J. CHRISTOPHER LYNCH IN
SUPPORT OF DEFENDANT'S MOTION FOR
ATTORNEYS' FEES - 110

"It's pretty clear what he has done, it is pretty clear what the results are," Pike responded.

"You've got problems if the numbers are not the correct numbers," Perram said. "You're going to have to fly him."

Perram ordered Dallas Buyers Club to fly the witness to Australia for cross-examination. The hearing of the case has been set down for late February.

ZDNet has again sought access to the expert report, after Perram [initially denied access](#) ([/article/how-dallas-buyers-club-gained-ip-addresses-locked-down-until-2015/](#)) to the report ahead of its being introduced into the court. Dallas Buyers Club opposed access to the report, while ISPs were not opposed, except for parts where IP addresses identifying customers were included.

Topics: [Piracy](#), [Australia](#), [Telcos](#)



About Josh Taylor

Armed with a degree in Computer Science and a Masters in Journalism, Josh keeps a close eye on the telecommunications industry, the National Broadband Network, and all the goings on in government IT.

[Contact](#)

Kick off your day with ZDNet's [daily email newsletter](#). It's the freshest tech news and opinion, served hot. [Get it.](#)

Join the discussion



colonel.mattyman

Dec 2, 2014

Catching pirates ...

It'll be interesting to see if the company the law firm used Maverickeye UG posted the movie up themselves to catch pirates given that notifications started arriving before the initial release date. If this is the case and the movie was authorised to be pirated, can they really go after people for downloading something that they themselves placed online and therefore authorised people to download?

[Like](#) [Reply](#)

Related Ads

1 [Home Security System](#)

2 [Cloud Storage](#)

3 [Free Microsoft Office](#)

4 [iPhone 6 Deals](#)

5 [Free Backup Software](#)

6 [Free Spyware Removal](#)

7 [CRM Solutions](#)

8 [Criminal Defense Lawyer](#)

[Quality Hearing Aids](#)

[iPhone 6 Deals](#)

[Malware Removal](#)

[Free Spyware Removal](#)

[Home Security System](#)



EXHIBIT E

SUPPLEMENTAL REPLY DECLARATION OF
J. CHRISTOPHER LYNCH IN
SUPPORT OF DEFENDANT'S MOTION FOR
ATTORNEYS' FEES - 113

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF INDIANA**

Dallas Buyers Club, LLC,

Plaintiff,

v.

DOES 1-20

Defendants

Case No. 1:14-cv-1142-WTL-MJD

DECLARATION OF DELVAN NEVILLE

1. My name is Delvan Neville. I am over the age of 21 and competent to execute this Declaration.
2. I am the owner of Amaragh Associates, LLC, a digital forensics company specialized in BitTorrent investigation. I am an ACE (AccessData Certified Examiner) as well as the author of a BitTorrent monitoring suite, EUPSC2k.
3. I was contacted by Gabriel J. Quearry of Quearry Law, LLC on October 8, 2014 in order to determine if I have previously performed monitoring of swarms associated with the Plaintiff and/or Crystal Bay Corporation (CBC), and whether or not a) records of such monitoring would establish the likelihood of a Doe defendant having been interconnected with a group of 20 IPs associated with the same infohash based on "hit dates" reported by CBC, and b) whether my records support allegations that it is IPP/GuardaLey performing the actual BitTorrent monitoring for Plaintiff, not CBC. I answered in the affirmative to both inquiries on October 8, 2014, and was provided with a copy of the initial complaint, the list of hit dates and the Declaration of Daniel Macek, and retained to provide a sworn declaration on my findings.
4. From mid-September through October 3rd of 2013, I performed BitTorrent monitoring and analysis work for the Electronic Frontier Foundation (EFF) meant to characterize the inter-connectivity of peers within a swarm¹. For these "soaks"², I monitored 24 swarms associated with IPP International-backed lawsuits, Crystal Bay Corporation (CBC) backed lawsuits, and swarms legally redistributing open-source software.
5. Though I had substantial pre-existing logs from soaks relating to both companies, I added new features to EUPSC2k for the purposes of this work to allow deep analysis of Peer Exchange protocol messages.
6. Peer Exchange (PEX) is an extended BitTorrent protocol whereby, following a handshake message between two peers, the peers will notify each other of the IPs of all other peers they are

1 Here, the term "swarm" is used as a generic label of all BitTorrent clients who are attempting to share a torrent with the same infohash at the same time. Because the infokey used to generate an infohash is not dependent on the list of trackers or attached to whether any peers use alternative means of finding other peers, a "swarm" is not necessarily a single interconnected collection of computers. The most overt example are private trackers i.e. the now-defunct Demonoid, which will only accept & share peer information for registered members of a given community, even if there are other individuals sharing a torrent with the same infohash with each other via a public tracker i.e. The Pirate Bay.

2 A "soak" is a continuous period of time during which one more EUPSC2k nodes are connecting to peers in a swarm to monitor and record their activity.

currently connected to within the same swarm, and subsequently update in later messages when any of those peers have disconnected. The purpose of PEX is to allow swarm members to discover each other in addition to the use of one or more trackers and/or Distributed Hash Table (DHT).

7. Through the use of PEX, I was able to not only characterize how long a typical swarm participant remained as a leecher³ and as a seeder⁴, but with what percentage of the observed swarm any PEX-enabled peer contacted during their lifetime in a swarm. Although the inter-connectivity of peers who do not support PEX cannot be directly observed, it stands to reason that peers that do not support this optional method to find more peers in a swarm will at the most be as equally interconnected as PEX-supporting peers, if not less so due to non-PEX peers having fewer options for finding new peers.
8. During the first soak, which consisted of a day long monitoring of 17 swarms of either IPP-monitored, CBC-monitored or legal (thus presumably unmonitored) swarms, the average time spent in a swarm as a leecher was 0.996 hours and the average time spent as a seeder was 3.117 hours, though both distributions had standard deviations approximately 3 times the value of the mean, indicating that both leeching time and seeding time are highly variable on an individual basis.
9. Based on a record of all IPs detected in each swarm by an EUPSC2k node and PEX communication by the subset of peers who report PEX data, the average peer contacts only 0.61% of the total number of swarm participants over the course of their time in the swarm, with a standard deviation of 1.35%. This indicates that a typical peer contacts only a sliver of all swarm participants, and while this distribution is also highly variable, 95% of swarm participants would have contacted between just a single peer to a maximum of 3.247%.
10. A second soak was performed on 7 more swarms, this time over a two-week period. This was directly inspired by mass-Doe litigation wherein the “hit dates”⁵ would often be days or weeks apart, rather than consisting of Does present in a swarm on the same day. The findings for time spent in the swarm were similar to those from the day-long soak: the average download time was 0.603 hours, and the average upload time 2.042 hours. As before, the standard deviations were large, in this case much larger (over 6 times the mean for both average download as well as upload times). Percent connectivity was an order of magnitude lower, however, at 0.05% on average with a standard deviation of 0.15%. This finding was not surprising, if peers only remain in the swarm for an average total of less than 3 hours, it is extraordinarily unlikely that peers from one day will have communicated with peers on a second day, let alone peers separated in time by weeks.
11. These results show that mass-joinder BitTorrent litigation is not based upon any real likelihood that the joined peers have engaged in any series of transactions with each other. Even if one were to assume that all 20 peers named in this suit were at the high end of the distribution of connectivity (3.247%), the likelihood that there is any series of peer-to-peer connections that could link all 20 peers together in the same series of transactions is 0.01%⁶.

3 A “leecher” as used here is a member of a swarm who has not yet finished downloading the contents of a torrent.

4 A “seeder” as used here is a member of a swarm who has finished downloading the contents of a torrent, but is still connected with members of the swarm, typically in order to continue to share the file(s) with others.

5 “Hit date” is used here only to coincide with the terminology used in IPP/CBC exhibits, and is not meant to endorse the concept that a “hit date” is an appropriate way to describe how and when a peer participated in a swarm.

6 This probability was calculated on the basis that any arrangement of communication that links each peer in this suit to at least one other peer would be sufficient. The probability is even more unlikely if there must be a contiguous series of links connecting all 20 peers through each other.

