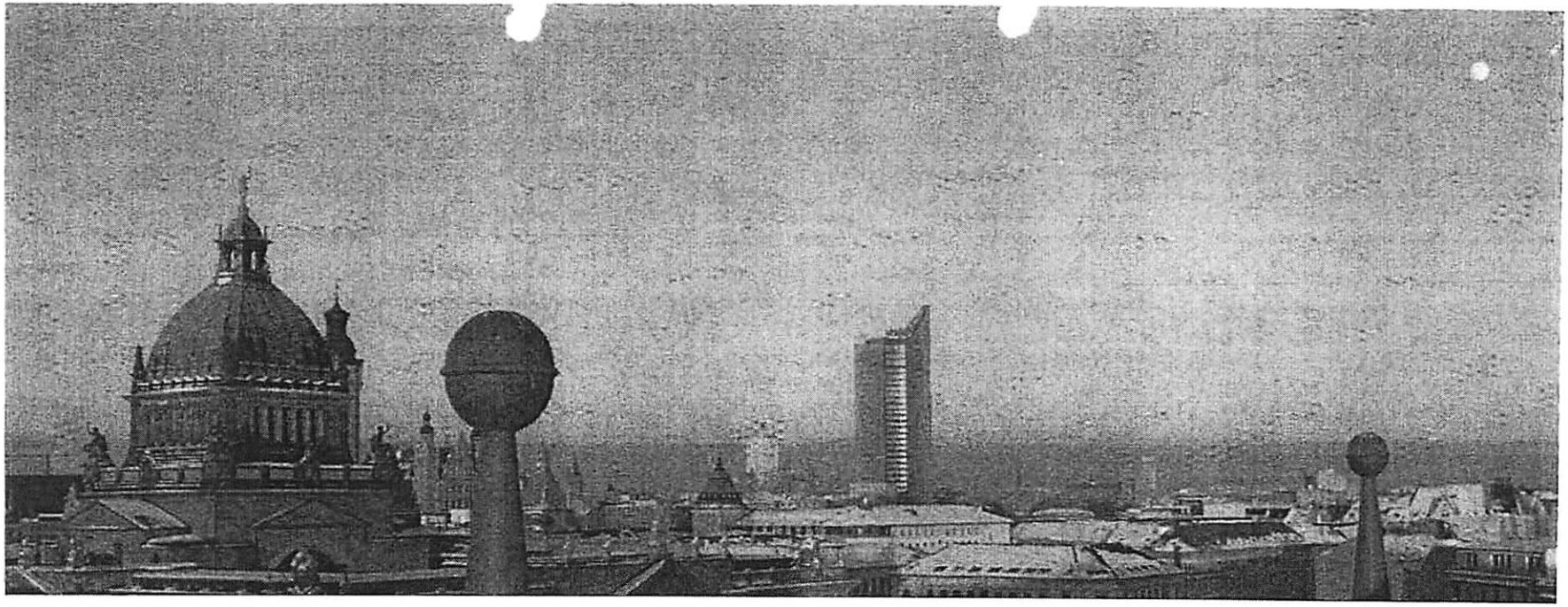

Fakten zur Abmahnung „Antichrist", BaumgartenBrandt an ipoque, 18.11.2009

CONFIDENTIAL
January, 2011

ipoque

Anlage AG 17

ipoque wurde für "Antichrist", das in einem Testscreening lief, abgemahnt

Fakten der Abmahnung

Abgemahnter:	**ipoque GmbH, Mozartstr. 3, 04107 Leipzig**
Abmahner:	**BaumgartenBrandt Rechtsanwälte, Berlin**
Bemerkung:	„Unabhängiger Sicherheitsdienstleister" ist Guardaley.
Mandantin:	**Zentropa Entertainments23 ApS**
Werk:	**Film „Antichrist"**
Datum, Zeit:	**18.11.2009, 01:03:25 MEZ**
IP-Adresse:	**79.222.120.152**
Bemerkung:	In dem fraglichen Zeitraum ist ein Testscreening mit diesem Film im externen Auftrag bei ipoque gelaufen. Die IP-Adresse war unsere. Es handelt sich um eine Datei im BitTorrent-Netzwerk (diese Information steht nicht im Abmahnschreiben).
Vorwurf:	**Angebot des Filmes zum Download durch Freigabe auf der Festplatte**
Gesamtbetrag:	**1200,- Euro**
Frist:	**18.05.2010**

Der Fall ist komplett aufgezeichnet und reproduzierbar

Fakten der Abmahnung

Der Fall konnte komplett nachvollzogen werden.

Dieses Testscreening lief auf dem PFS (Peer-to-Peer Forensic System), das ipoque selbst für Ermittlungen von Urheberrechtsverletzungen in Peer-to-Peer-Netzwerken einsetzt. Damit haben wir die kompletten Verkehrsmitschnitte aufgezeichnet und abgespeichert, der Fall kann also jederzeit wieder komplett nachvollzogen und belegt werden.

Wir haben den anderen Client (Guardaley) identifiziert

Der gegnerische Ermittler hatte zum fraglichen Zeitpunkt die IP-Adresse 78.43.254.8. Laut GoIP-Auskunft ist es Kabel Baden-Würtenberg, Karsruhe. Hinter dieser IP-Adresse standen in diesem Zeitraum von 21 Uhr am 17.11.2009 bis um 2 Uhr am 18.11.2009 insgesamt fünf verschiedene Clienthashes - einer pro angefragtem File. Wir haben damals diese fünf Files für Antichrist angefragt. Diese Informationen stehen nicht im Abmahnschreiben. Wir haben sie aus unserer Ermittlungsdatenbank analysiert:

ClientHash:	2D5554313831302D36D33E2627698192889A38D1
human readable:	-UT1810-6Ó%3E%26%27i%81%92%88%9A8Ñ
program and version:	-UT1810-

Der Guardaley-Client sendete ein charakteristisches Bitfeld

Fakten der Abmahnung

Wir haben nicht angeboten oder hochgeladen.

Unser Client hat weder ein Angebot gemacht, noch hochgeladen, da erstens unser P2P-Client allen anderen Clients mitteilt, das er nichts hat und der Client zweitens auch gar nichts hochladen könnte. Wir haben belegbar (in den kompletten Verkehrsmitschnitten) keinen einzigen Transfer an diesen Client gesendet.

Der Guardaley-Client hat nur angefragt, jedoch weder heruntergeladen, noch uns etwas gesendet – auch ipoque hat nichts transferiert

Die Clients der gegnerischen IP senden immer Bitfield 0101010101010101... (sie behaupten also immer jedes zweite und damit 50% des Files zu haben).

Screenshot 1 zeigt dieses Bitfeld.

Hinweis: Der Screenshot wurde mit Wireshark hergestellt, einem gängigen Programm zur manuellen Analyse von Netzwerkverkehr.

Screenshot 1: Bitfeld über die Verfügbarkeit von Pieces des gegnerischen Clients

78.43.254.8.erf - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: bittorrent.msg.bitfield Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
447	2009-11-18 00:40:59.004866660	78.43.254.8	79.222.120.152	BitTorrent	Bitfield, Len:0x57
467	2009-11-18 00:43:03.367750823	78.43.254.8	79.222.120.152	BitTorrent	Bitfield, Len:0x58
487	2009-11-18 00:48:24.049716413	78.43.254.8	79.222.120.152	BitTorrent	Bitfield, Len:0x58
504	2009-11-18 00:49:13.825836360	78.43.254.8	79.222.120.152	BitTorrent	Bitfield, Len:0x58
526	2009-11-18 00:53:27.782013059	78.43.254.8	79.222.120.152	BitTorrent	Bitfield, Len:0x55
543	2009-11-18 01:03:26.801057386	78.43.254.8	79.222.120.152	BitTorrent	Bitfield, Len:0x55
560	2009-11-18 01:08:04.129958272	78.43.254.8	79.222.120.152	BitTorrent	Bitfield, Len:0x57
583	2009-11-18 01:17:16.071639359	78.43.254.8	79.222.120.152	BitTorrent	Bitfield, Len:0x58
602	2009-11-18 01:20:32.125273943	78.43.254.8	79.222.120.152	BitTorrent	Bitfield, Len:0x57
621	2009-11-18 01:23:53.064983368	78.43.254.8	79.222.120.152	BitTorrent	Bitfield, Len:0xb0
639	2009-11-18 01:25:36.184803188	78.43.254.8	79.222.120.152	BitTorrent	Bitfield, Len:0x58
669	2009-11-18 01:34:28.032814264	78.43.254.8	79.222.120.152	BitTorrent	Bitfield, Len:0x58
689	2009-11-18 01:54:20.485980332	78.43.254.8	79.222.120.152	BitTorrent	Bitfield, Len:0x58
709	2009-11-18 01:56:44.456297159	78.43.254.8	79.222.120.152	BitTorrent	Bitfield, Len:0x57
726	2009-11-18 01:58:21.865115166	78.43.254.8	79.222.120.152	BitTorrent	Bitfield, Len:0x58
750	2009-11-18 02:00:51.109550595	78.43.254.8	79.222.120.152	BitTorrent	Bitfield, Len:0x57

```
    [Next sequence number: 91    (relative sequence number)]
    Acknowledgement number: 73    (relative ack number)
    Header length: 20 bytes
  ▷ Flags: 0x18 (PSH, ACK)
    Window size: 58589
  ▷ Checksum: 0x4fa0 [validation disabled]
  ▷ [SEQ/ACK analysis]
    [PDU Size: 98]
▽ BitTorrent
  ▽ Message: Len:86, Bitfield, Len:0x55
      Message Length: 86
      Message Type: Bitfield (5)
      Bitfield data: 55555555555555555555555555555555555555555555555555...
```

```
0000  00 15 17 15 d6 11 00 30  88 13 a6 da 81 00 69 07   .......0 ......i.
0010  88 64 11 00 19 80 00 84  00 21 45 60 00 82 48 89   .d...... .!E`..H.
0020  40 00 79 06 af 42 4e 2b  fe 08 4f de 78 98 12 75   @.y..BN+ ..O.x..u
0030  17 d1 73 fc 3f 1e 04 38  7f 67 58 18 e4 dd 4f a0   ..s.?..8 .gX...O.
0040  00 00 00 00 00 56 05 55  55 55 55 55 55 55 55 55   .....V.U UUUUUUUU
0050  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55   UUUUUUUU UUUUUUUU
0060  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55   UUUUUUUU UUUUUUUU
0070  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55   UUUUUUUU UUUUUUUU
0080  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55   UUUUUUUU UUUUUUUU
0090  55 55 55 55 55 55 55 55  55 55 55 54 74 dd d3 4e   UUUUUUUU UUUTt..N
```

Bitfield data (bittorrent.msg.bitfiel... Packets: 1060 Displayed: 55 Marked: 0 Profile: Default

Es hat niemals und in keiner Richtung ein Transfer stattgefunden

Fakten der Abmahnung

Der Screenshot 2 zeigt lückenlos den kompletten Vorgang zu der Abmahnung.

1: Es beginnt mit dem Handshake (Kontaktaufnahme durch den Gegner)
2: TCP Austausch (Bestätigung des Handshakepaketes, hat nichts mit dem Bittorrent-Vorgang zu tun) → es findet hier kein BitTorrent-Transfer o.ä. statt, es handelt sich nur um den Austausch zum Herstellen und Auflösen der TCP-Verbindung
3: Bestätigung des Handshakes durch uns
4: Gegner sendet (mutmasslich gefälschtes) Bitfeld (siehe Hinweis oben, Screenshot 1)
5: Unsere Antwort, das wir interessiert sind.
6: TCP (Bestätigung des Interested-Pakets im vorigen Schritt durch den Gegner)
7: Gegner fragt ein bestimmtes piece an (obwohl er weiss, das wir nichts haben, da wir kein Bitfeld gesendet haben – siehe Hinweis oben)
8: TCP Austausch (Bestätigung des Requestpakets durch uns)
9: Gegner fragt nochmals ein piece an
10: TCP (Bestätigung des Requestpakets durch uns)
11: TCP (Abbruch durch uns)
12: TCP (Bestätigung des Abbruchs durch Gegner)
13: TCP (Abbruch durch Gegner)
14: TCP (Bestätigung des Abbruchs durch uns)

Hinweis: Der Screenshot wurde mit Wireshark hergestellt, einem gängigen Programm zur manuellen Analyse von Netzwerkverkehr.

Screenshot 2: Der komplette abgemahnte Vorgang