



Оптимізація роботи з файлами resume.dat програмного забезпечення, що працює за протоколом BitTorrent

Іван Старенький

завідувач лабораторії досліджень об'єктів інформаційних технологій, телекомунікаційних систем (обладнання) та засобів, Одеський науково-дослідний інститут судових експертиз Міністерства юстиції України, м. Одеса, Україна, ORCID: <https://orcid.org/0009-0004-2271-8512>

У тезах наведено практичний спосіб покращення процесу дослідження файлів resume.dat, які є конфігураційними файлами програмного забезпечення, що працює за протоколом BitTorrent.

Ключові слова: торрент; скрипт; програмне забезпечення; файл.

Optimization of Working With Resume.dat Files in Software Operating via the Bittorrent Protocol

Ivan Starenkiy

The thesis presents a practical approach to improving the process of analyzing resume.dat files, which are configuration files used by software operating on the BitTorrent protocol.

Keywords: torrent; script; software; file.

Наше повсякденне життя сьогодні важко представити без постійного доступу до інтернету, починаючи від смарт-годинників та закінчуючи персональними та стаціонарними комп'ютерами. Спектр користувацьких запитів та сценаріїв звернення до інтернету всеосяжний: від робочих задач, перегляду серіалів та фільмів на online-сервісах на кшталт «Netflix», «Hulu», «Disney+», «HBO Max» до завантаження різноманітного контенту за допомогою програмного забезпечення (далі — ПЗ), що працює на архітектурі Peer-two-Peer (P2P) за протоколом «BitTorrent», до яких належать «qBitTorrent», «uTorrent», «Vuze», «Deluge», «BitLord», «Tizati», та ін.

Контент, який завантажується за допомогою наведених торрент-клієнтів, є як легітимним, так і забороненим на законодавчому рівні як для завантаження, так і для розповсюдження, наприклад, ст. 301 та 301-1 Кримінального кодексу України (далі — ККУ) [1].

Комп'ютерна техніка, якою скористались для завантаження та розповсюдження забороненого законом контенту, у майбутньому може стати об'єктом дослідження під час проведення судових комп'ютерно-технічних експертиз.

Незважаючи на те, що торрент-клієнти працюють за одним «BitTorrent»-протоколом, у них можуть бути різні програмні підходи до логування торрент-роздач у різні службові та конфігураційні файли, наведені

в GUI-середовищах (Graphical User Interface) торрент-клієнтів.

Так, наприклад, ПЗ «qBitTorrent» фіксує інформацію щодо торрент-роздач у декількох файлах: «*.fastresume», «*.torrent» (копії оригінальних торрент-файлів, що разом із fastresume-файлами зберігається в теці «BT_backup»), «qBittorrent-data.conf», «qBittorrent.ini» та «qBittorrent.log».

Водночас ПЗ «uTorrent» інформацію щодо роздач фіксує у файлах «resume.dat», «settings.dat», «*.torrent» (копії оригінальних торрент-файлів), «dht.dat», «rss.dat» та «*.log» (у разі, якщо було увімкнено логування). Поміж наведеного списку системних та конфігураційних файлів «resume.dat» є тим файлом, який містить максимально повну інформацію щодо роздач, усі інші файли також важливі для експертного дослідження, але все ж таки вони є другорядними. І саме тому дана робота присвячена оптимізації процесу дослідженню даного файлу.

Файл «resume.dat» містить таку інформацію щодо кожної торрент-роздачі: шлях до файлу / теки, ім'я торренту, відомості щодо статусу роздачі, прогрес завантаження, статистику UL/DL (downloaded, uploaded, ratio), часові мітки (added_on, completed_on, creation_date, active_time, seeding_time, last_seen_complete), кількість частин, параметр «piece_length», мітки, пріоритети файлів,

теги та параметри клієнта, *infohash*, розташування «*.torrent»-файлу.

Тому з позиції проведення комп'ютерно-технічної експертизи дослідження «*resume.dat*» та його інформаційного вмісту є важливою частиною дослідження.

У більшості випадків, коли постає питання дослідження файлу «*resume.dat*», то звертаються до ПЗ «BEncode Editor» [2], яке може працювати як з «*resume.dat*», так і з «*settings.dat*» та «*.torrent»-файлами (див. рис. 1—2).

Загалом ПЗ «BEncode Editor» — цілком гідний інструмент для встановлення відомостей щодо торрент-роздач, що зберігаються у файлі «*resume.dat*». За допомогою даного програмного продукту експерт може переглянути та перенести у свій висновок шляхом формування знімків робочої облас-

ті програмного продукту або копіюючи всі необхідні значення параметрів, що допоможуть сформувати відповіді на поставлені замовником запитання.

Але потрібно зазначити, що ПЗ «BEncode Editor» неспроможний вивантажувати інформацію щодо торрент-роздач, відомості про які містяться в «*resume.dat*», що у разі великої кількості раздач експоненціально збільшує час, який буде витрачено на оброблення інформації. Також робота з великим переліком раздач може призвести до того, що, ураховуючи людський чинник, деякі відомості щодо раздач, можливо навіть ключові, будуть пропущені через утому експерта від монотонних дій протягом тривалого часу.

Саме тому з метою уникнення помилок в «аналоговому» підході під час роботи з «*resume.dat*» автор розробив спеціальний

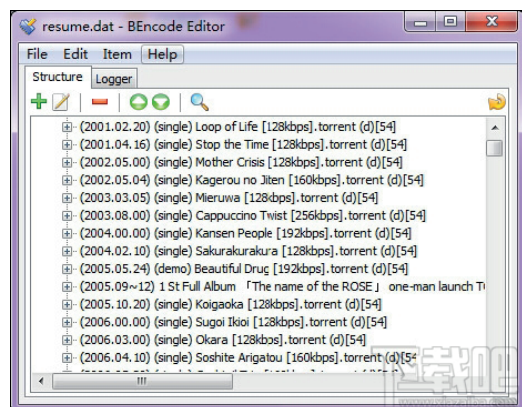


Рис. 1. Приклад робочого вікна ПЗ «BEncode Editor»

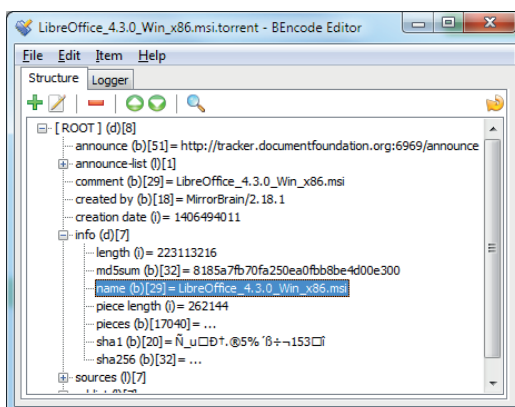


Рис. 2. Приклад перегляду інформації щодо торрент-роздачі в файлі «*resume.dat*»

Found 202 torrent(s):

```
-----
Name       : 03.02.14 MEM@OKC.mkv
Infohash   :
Path       : C:\Users\Павло\Downloads\03.02.14 MEM@OKC.mkv
Seeding    : False | Ratio None | UL/DL 1839366345/3491446985
UL/DL rate : None/None Limits UL/DL: None/None
Added/Done : 2014-02-04T20:59:44Z / 2014-02-04T21:22:17Z
Trackers   : http://bt3.rutracker.org/ann?uk=N9sxifyV1n, http://retracker.local/announce
-----
Name       : 13.j.rajon.Kirpichnye.osobnyaki.2014.RUS.BDRip.XviD.AC3.-HQCLUB.avi
Infohash   :
Path       : G:\13.j.rajon.Kirpichnye.osobnyaki.2014.RUS.BDRip.XviD.AC3.-HQCLUB.avi
Seeding    : False | Ratio None | UL/DL 2229616640/1559183360
UL/DL rate : None/None Limits UL/DL: None/None
Added/Done : 2014-10-12T15:35:51Z / 2014-10-12T15:47:34Z
Trackers   : http://bt2.rutracker.org/ann?uk=N9sxifyV1n, http://retracker.local/announce
-----
```

Рис. 3. Приклад результату роботи скрипту



Python-скрипт, що запускається в CLI-середовищі (*Command Line Interface*) операційної системи (ОС) «Linux» та взаємодіє з «*resume.dat*» файлом.

До функціональних можливостей скрипту включено автоматичний аналіз шляхом перебору всіх елементів файлу «*resume.dat*», тобто опрацювання інформації щодо

```
def scan_all_torrents(obj):
    found = []

    def walk(node):
        if isinstance(node, dict):
            for k, v in node.items():
                if isinstance(v, dict) and looks_like_torrent_dict(v, k):
                    ih = extract_infohash_from(v, k)
                    found.append(normalize_entry(ih, v))
                if isinstance(v, (dict, list)):
                    walk(v)
        elif isinstance(node, list):
            for it in node:
                walk(it)

    walk(obj)
    return found
```

Рис. 4. Рекурсивний пошук усіх торрент-записів у *resume.dat*

```
def looks_like_torrent_dict(d, key_bytes):
    if not isinstance(d, dict):
        return False
    h = d.get(b"hash")
    has_hash = isinstance(h, (bytes, bytearray)) and (len(h) == 20 or len(h) == 40)
    has_name = any(k in d for k in (b"name", b"caption", b"title"))
    has_path = any(k in d for k in (b"path", b"save_path"))
    key_looks_like_torrent = b".torrent" in key_bytes.lower()
    score = sum([has_hash, has_name, has_path, key_looks_like_torrent])
    return score >= 2
```

Рис. 5. Евристичне розпізнавання торрент-записів

```
def normalize_entry(infohash, entry):
    name = b2s(entry.get(b"name"))
    save_path = b2s(entry.get(b"save_path"))
    trackers = flatten_trackers(entry.get(b"trackers"))
    size = entry.get(b"size")
    downloaded = entry.get(b"downloaded")
    uploaded = entry.get(b"uploaded")
    added_on = maybe_ts(entry.get(b"added_on"))
    completed_on = maybe_ts(entry.get(b"completed_on"))
    return {
        "infohash": infohash.lower(),
        "name": name,
        "save_path": save_path,
        "trackers": trackers,
        "size": size,
        "downloaded": downloaded,
        "uploaded": uploaded,
        "added_on": added_on,
        "completed_on": completed_on,
    }
```

Рис. 6. Нормалізація одного запису про торрент-роздачу



торрент-роздач в автоматичному вигляді з подальшим збереженням результатів роботи у вихідний csv-файл (див. *рис. 3*).

Ураховуючи, що скрипт налічує більше 400 рядків програмного коду, в цій роботі наведено тільки деякі його ключові фрагменти (див. *рис. 4—6*).

Отже, застосування цього скрипту допоможе значно зберегти час на опрацювання інформації, що міститься в файлі «*resume.dat*», а завдяки можливості узагальнювати оброблений масив даних в один файл, він

робить скрипт потужним криміналістичним інструментом під час проведення комп'ютерно-технічних експертиз.

Перелік джерел посилання

1. Кримінальний кодекс України від 05.04.2001 р. № 2341-III (зі змін. та допов.). URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 26.01.2026).
2. BEncode Editor. URL: <https://sites.google.com/site/ultimasites/bencode-editor> (дата звернення: 26.01.2026).