Pedagogická fakulta
Faculty of Education

Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Jihočeská univerzita v Českých Budějovicích
Pedagogická fakulta
Katedra Informatiky

Bakalářská práce

Forenzní praxe při řešení informační kriminality z oblasti porušování autorských práv

Vypracoval: Jan Marek
Vedoucí práce: doc. Ing. Ladislav Beránek, CSc., MBA

České Budějovice 2014

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě - v úpravě vzniklé vypuštěním vyznačených částí archivovaných pedagogickou fakultou elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích 1. dubna 2014

.....
podpis

Abstrakt

Bakalářská práce „Forenzní praxe při řešení informační kriminality z oblasti porušování autorských práv “ se zabývá problematikou porušování autorských práv a příslušnou forenzní činností. V této práci bude popsán přehled právní úpravy trestního a autorského zákona a budou analyzovány možné způsoby páchání trestné činnosti z oblasti šíření a přechovávání autorsky chráněných produktů (software). Dále budou prozkoumány postupy forenzní praxe při řešení tohoto druhu informační kriminality. V praktické části provedu průzkum této problematiky ve zvolených organizacích, u širší veřejnosti a navrhnu automatizační metodu při získávání důkazních materiálů i při dokumentování. Vytvořím textový výstup s výsledky zjištěných informací.

Summary

The bachelor's thesis "The forensic practice in solving of informational criminality in the field - copyright violation" deals with the issue of copyright violation and the relevant forensic activity. In this thesis I will write about the juristic adjustment of the criminal and copyright law. I will analyse the possible way of the committing a crime - in the field of spreading and possesion copyrighteds (software).Then I will research the methods of the forensic practice during the solving the informational criminality. In my practical part I will research the choosen organisations and I will suggest the automation method during the gaining of the evidences. These will contain the text dokuments with my discovered information too.

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
Fakulta pedagogická
Akademický rok: 2012/2013

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan MAREK**
Osobní číslo:	**P11056**
Studijní program:	**B7507 Specializace v pedagogice**
Studijní obor:	**Informační technologie a e-learning**
Název tématu:	**Forenzní praxe při řešení informační kriminality z oblasti porušování autorských práv**
Zadávající katedra:	**Katedra informatiky**

Zásady pro vypracování:

Práce se zaměří na oblast porušování autorských práv a příslušné forenzní činnosti. V teoretické části bude proveden přehled právní úpravy trestní a autorského zákona, bude analyzovat možné způsoby páchání trestné činnosti z oblasti šíření a přechovávání autorsky chráněných produktů (software). Dále prozkoumá postupy forenzní praxe při řešení tohoto druhu infor...ační kriminality. V praktické části provede průzkum této problematiky ve zvolených organizacích a navrhne automatizační metodu při získávání a dokumentaci důkazních materiálů včetně vytvoření textového výstupu s výsledky zjištěných informací.

Rozsah grafických prací: CD ROM

Rozsah pracovní zprávy: 40

Forma zpracování bakalářské práce: tištěná

Seznam odborné literatury:

1. Autorský zákon. In: 121/2000. 7. dubna 2000
2. COWEN, David. Computer forensics: infoSec Pro guide. pages cm. ISBN 978-007-1742-450.
3. Místo a úloha forenzní analýzy IS. In: RAC - White Paper [online]. 2002 [cit. 2013-04-10]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/Download/$FILE/Forenz_audit.pdf
4. LIMBERK, Tomáš. Forenzní vědy a jejich využití v kriminalistice. Brno, 2011. Bakalářská práce. Právnická fakulta Masarykovy univerzity.
5. COWEN, David. Computer forensics: infoSec Pro guide. 1. vyd. Boston: McGraw-Hill Osborne Media, 2013, pages cm. ISBN 978-007-1742-450.
6. KRUSE, Warren G a Jay G HEISER. Computer forensics: incident response essentials. Boston, MA: Addison-Wesley, 2001, xiii, 392. ISBN 02-017-0719-5.

Vedoucí bakalářské práce: **doc. Ing. Ladislav Beránek, CSc.**
Katedra aplikované matematiky a informatiky

Datum zadání bakalářské práce: **16. dubna 2013**

Termín odevzdání bakalářské práce: **30. dubna 2014**

Mgr. Michal Vančura, Ph.D.
děkan

L.S.

doc. PaedDr. Jiří Vaníček, Ph.D.
vedoucí katedry

V Českých Budějovicích dne 16. dubna 2013

Klíčová slova

Forenzní praxe při řešení informační kriminality, forenzní analýza, licenční podmínky, trestní zákon, autorský zákon.

Keywords

The forensic practice in solving of informational criminality, forensic analysis, license terms, the criminal law, the copyright laws.

Poděkování

Zde bych chtěl poděkovat doc. Ing. Ladislavu Beránkovi, CSc., MBA za odborné rady při tvorbě této práce.

Obsah

1 Úvod a cíle práce

1.1 Úvod

Autorské právo je velmi častým tématem mezi právníky, policií a veřejností. Mnoho lidí si neuvědomuje závažnost porušení licenčního ujednání. Mnohdy se jedná o nedostatečné znalosti, které způsobí obrovské škody na majetku tvůrce a zároveň vysoké sankce a tresty na straně pachatele.

Mezi roky 2000 a 2005 byl nárůst informační kriminality softwaru o více než 160 % a následně až do roku 2010 rostl. Nyní se tento trend krádeže pozastavil a začíná se velmi pomalu zlepšovat. Z průzkumu statistického úřadu vyplývá, že kolem 70 % občanů České republiky vlastní osobní počítač a používá internet. Přičemž nejvíce krádeží softwaru a licenčních produktů se stává právě na internetu a dochází zde mnohdy i k organizovanému zločinu.

V práci se zaměřím na oblast porušování autorských práv a příslušnou forenzní činnost. Práce bude obsahovat jak teoretickou, tak praktickou část. V teoretické části shrnu přehled právní úpravy trestního a autorského zákona, budu analyzovat možné způsoby páchání trestné činnosti z oblasti šíření a přechovávání autorsky chráněných produktů (software). Dále budu zkoumat postupy forenzní praxe při řešení tohoto druhu informační kriminality. V praktické části provedu průzkum této problematiky mezi informačními experty i širší veřejností. Dále navrhnu optimální metodu získávání dat z bitové kopie disku, výsledkem bude textový výstup do tabulkového editoru a vytvoření výsledného ukázkového reportu.

1.2 Cíle práce

- Přehled právní úpravy trestního a autorského zákona
- Způsoby páchání trestné činnosti a přechovávání autorsky chráněných produktů
- Hardwarový a softwarový audit počítačů
- Zkoumání forenzní praxe při řešení autorského práva informační kriminality

- Navrhnutí optimálního postupu získávání dat o nelegálním přechovávání licenčních produktů
- Návod na použití navrženého postupu
- Průzkum mezi širší veřejností a IT experty na téma informační kriminalita zaměřený na licenční ujednání

2 Přehled autorského a trestního zákona k dané problematiky

Zde bych shrnul autorské a trestní právo vztahující se k informační kriminalitě. Několik důležitých paragrafů a odstavců, které jsou nezbytné k pochopení a vysvětlení informační kriminality a licenčních podmínek.

2.1 Autorské právo a práva s ním související

Důležité výňatky z platného znění zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským. Co je označeno jako autorské dílo podle aktuálního autorského zákona s poslední změnou v roce 2013, dle § 2 písm. a) zákon č. 121/2000 Sb.

2.1.1 Autorské dílo

(1) Předmětem práva autorského je dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam (dále jen "dílo"). Dílem je zejména dílo slovesné vyjádřené řečí nebo písmem, dílo hudební, dílo dramatické a dílo hudebně dramatické, dílo choreografické a dílo pantomimické, dílo fotografické a dílo vyjádřené postupem podobným fotografii, dílo audiovizuální, jako je dílo kinematografické, dílo výtvarné, jako je dílo malířské, grafické a sochařské, dílo architektonické včetně díla urbanistického, dílo užitého umění a dílo kartografické. *(Přepisy zákonů, 2013)*

Z prvého odstavce autorského zákona je zřejmé, že jakákoliv fotografie, píseň a video je majetkem autora díla. Z toho vyplývá, že na jakékoliv stažení například fotografie, písně, videoklipu, či filmu potřebujeme autorovo souhlas, pokud jej neposkytuje širší veřejnosti zcela zdarma.

(2) Za dílo se považuje též počítačový program, je-li původní v tom smyslu, že je autorovým vlastním duševním výtvorem. Databáze, která je způsobem výběru nebo uspořádáním obsahu autorovým vlastním duševním výtvorem a jejíž součásti jsou systematicky nebo metodicky uspořádány a jednotlivě zpřístupněny elektronicky či jiným způsobem, je dílem souborným. Jiná kritéria pro stanovení způsobilosti

počítačového programu a databáze k ochraně se neuplatňují. Fotografie a dílo vyjádřené postupem podobným fotografii, které jsou původní ve smyslu věty první, jsou chráněny jako dílo fotografické. *(Přepisy zákonů, 2013)*

Z druhého odstavce je patrné, že autorský zákon se samozřejmě vztahuje na vytvořený software. To znamená, že jakýkoliv software, který náleží autorovo duševnímu výtvoru, je chráněn autorským právem pro majitele. Jednoznačně zde platí, že jakýkoliv program je trestné stahovat, nebo jakkoliv kopírovat, pokud autor neposkytuje produkt zcela zdarma, nebo ve verzi demo, či s omezenou platností používání.

(3) Právo autorské se vztahuje na dílo dokončené, jeho jednotlivé vývojové fáze a části, včetně názvu a jmen postav, pokud splňují podmínky podle odstavce 1 nebo podle odstavce 2, jde-li o předměty práva autorského v něm uvedené. *(Přepisy zákonů, 2013)*

(4) Předmětem práva autorského je také dílo vzniklé tvůrčím zpracováním díla jiného, včetně překladu díla do jiného jazyka. Tím není dotčeno právo autora zpracovaného nebo přeloženého díla. *(Přepisy zákonů, 2013)*

Z odstavce třetího a čtvrtého autorského zákoníku nám vyplívá, že dílo nemusí být dokončeno a již se považuje za trestné ho kopírovat, šířit a používat bez souhlasu majitele. Zároveň jakýkoliv překlad a vzniklým tvůrčím dílem jiného autora, se nepovažuje jako trestní čin, porušení autorského práva.

2.1.2 Výjimka o autorském díle

Dle nejnovější i starší verze zákoníku se nepovažuje za autorské dílo, na které lze uplatňovat autorský zákon, mnoho listin a děl. Ve velké míře se jedná o listiny vydané úřady, různé předpisy, veřejné sbírky, listiny a další díla. Do této výjimky patří i výtvory tradičních lidových kultur, kde není znám autor a zároveň neznehodnocujeme daný obsah díla.

2.1.3 Autor

V druhém dílu zákoníku se dočteme, kdo může být autorem, v našem případě softwaru a médií. Zde bych vyzdvihl pouze základní definici autora. Samozřejmě může být autorů více, mohou vystupovat pod pseudonymy atd.

(1) Autorem je fyzická osoba, která dílo vytvořila. *(Přepisy zákonů, 2013)*

(2) Autorem díla souborného je fyzická osoba, která je tvůrčím způsobem vybrala nebo uspořádala; tím nejsou dotčena práva autorů děl do souboru zařazených. *(Přepisy zákonů, 2013)*

2.1.4 Vznik autorského práva

Ve třetím dílu, prvém oddílu a devátém paragrafu je definováno nabytí autorského práva na dílo.

(1) Právo autorské k dílu vzniká okamžikem, kdy je dílo vyjádřeno v jakékoli objektivně vnímatelné podobě. *(Přepisy zákonů, 2013)*

(2) Zničením věci, jejímž prostřednictvím je dílo vyjádřeno, nezaniká právo autorské k dílu. *(Přepisy zákonů, 2013)*

(3) Nabytím vlastnického práva nebo jiného věcného práva k věci, jejímž prostřednictvím je dílo vyjádřeno, nenabývá se oprávnění k výkonu práva dílo užít, není-li dohodnuto či nevyplývá-li z tohoto zákona jinak. Poskytnutím oprávnění k výkonu práva dílo užít jiné osobě zůstává nedotčeno vlastnické právo nebo jiná věcná práva k věci, jejímž prostřednictvím je dílo vyjádřeno, není-li dohodnuto či nevyplývá-li ze zvláštního právního předpisu jinak. *(Přepisy zákonů, 2013)*

(4) Vlastník či jiný uživatel věci, jejímž prostřednictvím je dílo vyjádřeno, není povinen tuto věc udržovat a chránit před zničením, není-li dohodnuto či nevyplývá-li ze zákona jinak. *(Přepisy zákonů, 2013)*

2.1.5 Správní delikty – přestupky

Hlava VI, kapitola Správní delikty, autorského zákona, přesněji § 105a přesně popisuje, kdy se dopouštíme přestupku při porušení zákona.

(1) Fyzická osoba se dopustí přestupku tím, že:

a) neoprávněně užije autorské dílo, umělecký výkon, zvukový či zvukově obrazový záznam, rozhlasové nebo televizní vysílání nebo databázi,

b) neoprávněně zasahuje do práva autorského způsobem uvedeným v § 43 odst. 1 nebo 2 anebo v § 44 odst. 1, nebo

c) jako obchodník, který se účastní prodeje originálu díla uměleckého, nesplní oznamovací povinnost podle § 24 odst. 6. *(Přepisy zákonů, 2013)*

2) Za přestupek podle odstavce 1 písm. a) lze uložit pokutu do 150 000 Kč, za přestupek podle odstavce 1 písm. b) pokutu do 100 000 Kč a za přestupek podle odstavce 1 písm. c) pokutu do 50 000 Kč. *(Přepisy zákonů, 2013)*

2.1.6 Rozšiřování

Ve čtrnáctém paragrafu se dočteme o šíření a právech majitele na originál. Zde jednoznačně vyplývá, pokud autor software nebo média se rozhodne jej rozšiřovat a nabídne jej k prodeji, neztrácí na něj autorské právo a každá kopie je jeho majetkem, pokud není prodána. S tím souvisí licencování softwaru. Z § 46 je patrné, že pokud tvůrce uvalí na daný produkt z oblasti informatiky licenční ujednání, stává majitelem. Licence se dále ještě dělí na výhradní a nevýhradní, kde se jedná ale pouze už o rozhodnutí majitele, jak bude například software distribuovat. Z přečtení autorského zákona jednoznačně vyplívá, že software je právoplatným produktem.

2.2 Trestné právo důsledkem informační kriminality

Důsledkem nelegálního šíření software nebo mediálních soborů jakýmkoli způsobem se šiřitel dopouští přestupku či trestného činu krádeže. Lze ho trestat dle platného trestního zákoníku č. 40/2009 Sb.

„Žádný trestný čin bez zákona.“ (Jelínek & etc. ALL, 2013)

Důležitá kapitola trestního zákoníku k tématu informační kriminality z oblasti porušování autorských práv se nazývá Trestné činy proti průmyslovým právům a proti autorskému právu, především § 268, porušení práv k ochranné známce a jiným označením.

2.2.1 Porušení práv k ochranné známce a jiným označením

(1) Kdo uvede do oběhu výrobky nebo poskytuje služby neoprávněně označené ochrannou známkou, k níž přísluší výhradní právo jinému, nebo známkou s ní zaměnitelnou nebo pro tento účel sobě nebo jinému takové výrobky nabízí, zprostředkuje, vyrobí, doveze, vyveze nebo jinak opatří nebo přechovává, anebo takovou službu nabídne nebo zprostředkuje, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty. *(Jelínek & etc. ALL, 2013)*

(2) Stejně bude potrestán, kdo pro dosažení hospodářského prospěchu neoprávněně užívá obchodní firmu nebo jakékoliv označení s ní zaměnitelné nebo uvede do oběhu výrobky nebo služby neoprávněně opatřené označením původu nebo zeměpisným označením anebo takovým označením s ním zaměnitelným nebo pro tento účel sobě nebo jinému takové výrobky nebo služby nabídne, zprostředkuje, vyrobí, doveze, vyveze nebo jinak opatří nebo přechovává. *(Jelínek & etc. ALL, 2013)*

(3) Odnětím svobody na šest měsíců až pět let, peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,

a) získá-li činem uvedeným v odstavci 1 nebo 2 pro sebe nebo pro jiného značný prospěch, nebo *(Jelínek & etc. ALL, 2013)*

b) dopustí-li se takového činu ve značném rozsahu.

(4) Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) získá-li činem uvedeným v odstavci 1 nebo 2 pro sebe nebo pro jiného prospěch velkého rozsahu, nebo

b) dopustí-li se takového činu ve velkém rozsahu. (Jelínek & etc. ALL, 2013)

2.2.2 Porušení autorského práva, práv souvisejících s právem autorským

Nejdůležitější paragraf pro porušení autorského zákona v trestním zákoně je § 270 porušení autorského práva, práv souvisejících s právem autorským a práv k databázi.

(1) Kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty. *(Jelínek & etc. ALL, 2013)*

(2) Odnětím svobody na šest měsíců až pět let, peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,

a) vykazuje-li čin uvedený v odstavci 1 znaky obchodní činnosti nebo jiného podnikání,

b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch nebo způsobí-li tím jinému značnou škodu, nebo

c) dopustí-li se takového činu ve značném rozsahu. (Jelínek & etc. ALL, 2013)

(3) Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu nebo způsobí-li tím jinému škodu velkého rozsahu, nebo

b) dopustí-li se takového činu ve velkém rozsahu. (Jelínek & etc. ALL, 2013)

Dle trestního zákonu viník, který se dopustí trestného činu porušování autorských práv v oblasti informatiky týkající se softwaru a médií, může dostat délku trestu nepodmíněně až na osm let.

3 Licence

Základním principem licence je chránění produktu. Při koupi softwaru si nekupujeme daný program, ale licenci produktu. Tudíž nekupujeme samotný software, ale pouze práva k užívání daného programu. Součástí každého originálního produktu je i instalační médium a manuál, ale hlavním prodávaným předmětem je nehmotný majetek, tudíž licence programu.

S tímto jsou spjaté další důležité informace ohledně nakládání s programem se zakoupenou licencí. Výrobce jednotlivých softwarů může stanovit jednotlivá omezení pro používání a nakládáním se softwarem. Je velmi dobré znát jednotlivá omezení a důkladně si přečíst licenční podmínky, protože pokud nějaké z výrobcem stanovených pravidel poruším, může to mít nemalé následky.

Software je i po zakoupení uživatelem stále majetkem výrobní společnosti. Ve skutečnosti si uživatel jako koncový zákazník kupuje pouze právo na užívání produktu za předem daných obchodních podmínek.

Také je velmi důležité odlišovat samostatný software a nosič, na kterém je zaznamenán. I skutečnost, že jsme vlastníkem nosiče daného programu, neznamená, že daný produkt můžeme využívat. V konečné fázi je vytvořený software stále majetkem výrobní společnosti, pouze ho poskytuje k užívání jednotlivým uživatelům s předem jasně stanovenými pravidly. Koncový zákazník se tudíž nestává majitelem softwaru ani licenčních práv k němu, ale pouze majitelem licence programu.

Licenční smlouva shrnuje majitelem předepsané podmínky pro jednotlivé uživatele. Pokud s nimi uživatelé nesouhlasí, znamená to, že nemůžou užívat tento produkt ve svůj prospěch. Akceptování licenčních podmínek u softwaru se v největší míře potvrzuje stiskem tlačítka „souhlasím“. Pokud uživatel tento krok akceptuje, souhlasí s licenčními podmínky a zavazuje se tak k jejich dodržování. Neseznámení se s licenčními podmínkami a následné potvrzení tlačítka „souhlasím“, je nejčastější chyba, kvůli které dochází k nelegálnímu užívání softwaru a následnému porušování autorského práva. Bohužel neznalost neomlouvá, všechny následky jdou poté za uživatelem.

Při akceptování licenčních podmínek se většinou zavazujeme, že nebudeme software rozšiřovat, napodobovat a zneužívat. Tímto krokem poté mohou majitelé produktů při porušení práv uživatelem podat trestní oznámení, jelikož se jim uživatel zavázal k licenčním podmínkám spjatým k softwaru.

3.1 Možnosti zakoupení licencí

Lokální licence

K programu nebo k souborům programů je přidělen a dodáván jeden hardwarový klíč, který pomáhá určovat, jaké programy mají pracovat v licenční verzi. Programy fungují pouze v případě, že je k počítači připojený hardwarový klíč.

Síťová licence

K souboru programů je dodáván síťový hardwarový klíč. Programy lze ovládat z libovolného počítače v síti. Nelze jej spouštět několika uživateli najednou, v takovém případě by se musela pořídit multilicence.

Multilicence

Bývá dodávána s několika klíči nebo s jedním síťovým klíčem. Multilicence je vytvářena jen na jeden objekt. Následující licence nemusejí obsahovat všechny programy, které jsou zakoupeny na základní licenci.

Vzdělávací licence

Tato licence je určena pouze pro výukové účely, je zakázáno ji komerčně používat a může ji zakoupit pouze jakákoliv vzdělávací instituce.

Studentská licence

Určená pouze pro registrované studenty. Nesmí se používat komerčně ani jakkoliv zneužívat tímto směrem. Slouží k vytváření a používání výukových materiálů v instituci. K souborům je dodáván hardwarový klíč s omezenou platností, který aktivuje programy. Často se zde skládá záloha, která je po vrácení klíče zaslána zpět studentovi.

3.2 Vybrané typy licencí

3.2.1 Ukázka typů licencí

Adware	Freeware pro nekomerční využití	PHP Licence
Apache Licence	IPL	Pine Licence
2.0Artistic Licence	LGPL	Plná verze
Cardware	MIT Licence	Public Domain
Creative Commons	GNU	SCSL
Demo	GPL	Shareware
DJB	MPL	SISSL
Donationware	MS EULA	SPL
EULA	NPL	Start
Freeware	Open Publication Licence	Trial
Orphanware	PDL	W3C dokument Licence

3.2.2 Nejčastější typy licencí

Adware – Užívání programu s tímto typem licence je bezplatné, ale součástí je vložená reklama, která financuje vývoj programu. Reklamu dle licenčního ujednání je zakázáno jakkoliv odstraňovat.

Freeware – pod touto licencí se rozumí volně šiřitelný program. Autor poskytuje program k užívání zcela zdarma a ponechává si autorské právo. Program se nesmí jakkoliv upravovat, bez souhlasu majitele ani nijak dále šířit s úmyslem výdělku. Majitel program vytváří spíše pro vlastní uspokojení než se záměrem zisku.

EULA – Než produkt nainstalujete, musíte souhlasit s licenčními podmínky výrobce. Používaná licence například giganta Microsoft.

GNU GPL - General Public License, software s touto licencí lze bezplatně používat i šířit. Nelze ho šířit s úmyslem výdělku. Můžete se dostat bezplatně ke zdrojovým kódům a upravit podle svého. Na programy s touto licencí se nevztahuje záruka ani licence schválená sdružením OSI.

Shareware – Program s licencí shareware je distribuován zdarma, každý si jej může stáhnout. Majitel požaduje malý poplatek po uživatelích, kteří program využívají aktivně, kteří chtějí dostávat automatické aktualizace či mají k dispozici online podporu. Poplatek je na rozdíl od ostatních typů placených licencí banální. Díky šíření přes internet je to velmi často používaná licence.

Public domain – Autor se vzdává práv na svůj produkt. Lze jej volně šířit, používat, upravovat i používat pro svou tvorbu do aplikací.

Trial – Velmi omezená verze komerčního softwaru, která je nejčastěji časově omezená. Vyskytují se zde zakázané některé funkce, které se aktivují až po zakoupení plné verze programu. S trial licencí si stáhneme nejčastěji demo verzi, která je rovněž časově omezená.

SCSL – Velmi omezená licence a také problematická. Setkáváme se sní například u Java 2 – JDK a JRE. Nelze distribuovat dílo dále pod touto licencí. Schváleno sdružením OSI.

4 Způsoby páchání trestné činnosti

Porušování autorského práva je v dnešní době „tolerováno“ a pro některé je to každodenní záležitost. Mnoho takových lidí si neuvědomuje, že porušují zákon a způsobují nemalé škody. Poškozený majitel poté po nich požaduje odškodnění za ušlý zisk a způsobené škody. Jen v letošním roce máme dvě velké kauzy na území České republiky. Hříšníci pocházející z Jižních Čech a z Moravy, způsobily celkem škody přesahující 110 milionu korun.

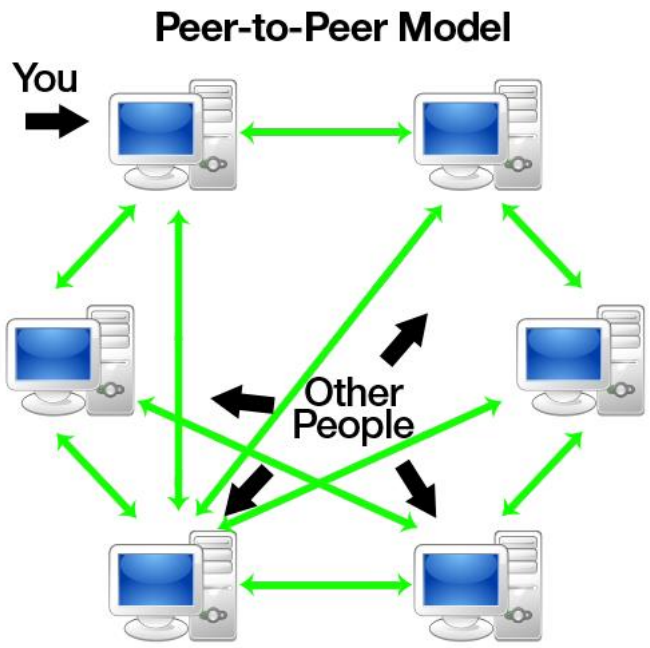
Trend nelegálního stahování a obcházení bezpečnostních prvků každoročně narůstá. Nejedná se přitom o stahování pouze softwaru, ale i filmů a hudby. Důvodem je zejména rozvoj digitálních technologií v posledních letech a jejich všeobecná rozšířenost a snadná dostupnost široké veřejnosti spolu s „neuchopitelností“ duševního vlastnictví a tím i snazšímu ospravedlnění protiprávního jednání. Snadné a bezpracné šíření chráněných děl v masivním měřítku zejména prostřednictvím peer to peer (P2P) sítí a filehostingových a FTP serverů pak umožnil především internet. Hlavním důvodem masivního porušování autorských práv, které technologický pokrok jenom usnadnil a učinil jednoduše dostupným široké veřejnosti, je především dlouhodobě celospolečensky zakořeněná nízká úcta k právům duševního vlastnictví. Z hlediska samotných porušovatelů práv i značné části společnosti není pirátství vnímáno jako nemorální, závažné či poškozující, ale spíše jako běžné, pochopitelné a ospravedlnitelné jednání, max. džentlmenský delikt. *(Lenka Hečková, 2008)*

4.1 Peer to peer (P2P) sítě

Peer to peer neboli „rovný s rovným“ - tyto sítě jsou založené na vzájemné komunikaci jednotlivých uživatelů. Hlavní rozdíl oproti normálnímu připojení pomocí internetu, kde se nejčastěji připojujete na server a kde jsou uložené obrázky, videa i celé weby je ten, že zde se připojují jednotliví uživatelé pouze mezi sebou a vyměňují si tak informace přímo. V peer to peer síti nejsou žádná centra. Existují samozřejmě výjimky, ty slouží ale především k usnadnění komunikace. Všichni se tedy připojují k sobě navzájem. U P2P je velmi důležitá rychlost, na rozdíl od připojení klient –

server platí, čím více připojených klientů, tím menší rychlost. U P2P je to zcela naopak, čím více lidí v komunitě, tím větší rychlost.

Typické je pro tuto architekturu využití torrentů. Přes ně uživatelé sdílejí různé soubory typu hudby, filmů, SW a jiné, bohužel mnohdy ilegálně. Hierarchie využití P2P sítě je jednoduchá, pokud chcete něco stáhnout z internetu pomocí této sítě, musíte zároveň i něco nabídnout ke stažení ostatním. A to už je v rozporu se zákonem.



Obr1. Model Peer to peer (Jalilifard, 2013)

4.2 File hosting server

Službu file hosting server lze definovat jako datová uložiště na internetu, která umožňují dopravit data ke všem uživatelům, tudíž „sdílení“. V nynější době zde máme mnoho nabídek, kam své data uložit. Ve valné většině můžeme omezený počet megabit vložit zcela zdarma u těchto typů serverů. Důležitým parametrem je rychlost přenosu dat. Pokud bychom chtěli využít větší kapacitu serveru, pokročilé funkce vkládání a správy bývají tyto služby zpoplatněny. Na těchto typech serverů se

nachází mnoho produktů, u kterých vkládající uživatel porušuje licenci produktu. Poté se bavíme o nezákonném šíření.

4.3 FTP server

FTP server (file transfer protocol) využívá přenos mezi jednotlivými počítači pomocí počítačové sítě. Tento protokol je z rodiny TCP/IP, je zde používán model „klient - server“. Uživatel se připojí k serveru pomocí FTP protokolu a může provádět mnoho operací, které jsou definovány ve FTP protokolu. Můžeme zde vytvářet klienty pro jakékoliv prostředí. Na internetu je mnoho dostupných programů i ve verzi freeware pro FTP servery i klienty.

V novější verzi operačního systému Windows, vepsáním příkazu „cmd“ do pole spustit a následném vepsání FTP a odesláním, se můžete připojit k serveru. Konkrétněji příkazem „open název serveru“. Nejčastějším využitím je samozřejmě sdílení dat a správa internetových stránek. Často se také využívá tento přenos k přístupu na vzdálený počítač. Nevýhody spočívají v nešifrovaném zasílání hesla při přihlášení. Lze jej dodatečně šifrovat. Při využívání firewall vyžaduje protokol speciální podporu, nefunguje u šifrovaného aktivního přenosu. Celkově má FTP server delší odezvu a není tak často využíván. Mezi velkou nevýhodu patří nešifrování hesla, kde pak může dojít ke katastrofálním ztrátám, jestliže zachytí heslo třetí strana. Na těchto typech uložišť se nachází mnoho dat, která jsou v mnoha případech i autorsky chráněná.

4.4 Nástroje a postupy při porušování licence

4.4.1 Bezpečnostní prvky

Registrační číslo (serial number) je nejčastější typ ochrany softwaru, setkáváme se s ním téměř všude. Dnes není problém ho překonat, tudíž není moc spolehlivým bezpečnostním prvkem. Nejčastější a také nejbezpečnější formou zabezpečení je přidělení registračního čísla s číslem pevného disku. V dnešní době se objevuje také online generování čísla přes internet, bohužel v tom vidím znevýhodnění.

Časové omezení (time trial) je často spjaté se sériovým číslem. Po zadání správného sériového čísla se časové omezení zruší. Opět tato metoda zabezpečení

není moc spolehlivá. Pokud pokročilý uživatel změní API funkci nebo v kódu najde metodu, která získává aktuální čas, lze snadno překonat toto zabezpečení. Časové omezení musí získávat informaci o aktuálním čase.

Klíčový soubor (key file) je jedna z nejbezpečnějších forem zabezpečení. Klíčový soubor může obsahovat část programu či klíč pro dekomprimování při startu programu. Toto zabezpečení bývá taktéž kombinováno s časovým omezením, po nahrání klíčového souboru dojde k odblokování časového omezení. Vytvoření klíčového souboru pro prolomení nezvládne jen tak nějaký expert na počítače. Využívají se zde funkce API jako CreateFile, ReadFile, WriteFile, SetFilePointer.

Hardwarový klíč (dongle) je další metoda, která patří mezi nejbezpečnější. Pokud je správně nakonfigurována, je téměř nepřekonatelná. Hacker by musel simulovat hardwarový klíč či ho nějak obdobně vyrobit. Ale i proti softwarovému prolomení se zde může výrobce chránit. Vyrobení klíče je velmi nákladné pro crackera. V dnešní době je nejčastější využití přes USB. Nejznámější hardwarové klíče jsou typu HASP a Sentinel.

Kontrola originálního CD (CD-check) - dříve zbytečná záležitost. V dnešní době, při porovnání ceny CD a vypalovací mechaniky, je kontrola CD nezbytnou součástí zabezpečení. Nejčastějším systémem zabezpečení jsou „errory“ schválně vložené na CD, které tak zabraňují kopírování a šíření. Vyhazují chybové hlášky např. u vypalování. Pokud se budeme bavit o hře na PC, hra se může vypínat a chovat se nestabilně. Tento druh ochrany vynalezla společnost SONY.

Demo je asi každému známá verze. Distribuce je zdarma. Velmi ořezaný produkt, kde je účelem nahlédnutí zákazníka, aby věděl, o jaký software nebo hru jde. Jediná možnost, jak docílit plné funkčnosti, je si koupit plnou verzi aplikace či hry.

Ochrana naprogramovaná ve Visual Basicu nebo Delphi - zde je samotná ochrana programovací jazyk. Kód je převeden do pseudoinstrukcí a je velmi složité ho cracknout. Většinu času by trávil cracker v systémových knihovnách. Proto je velmi unikátní se setkat s cracknutým programem tohoto typu.

Komprese a kódování programů - tato metoda zabezpečení se využívá téměř u každého programu, krom typu freeware a OpenSource. Metoda jednoduše šifruje, komprimuje program.

4.4.2 Hacker

Počítačový piráti a specialisté na informatiku dokážou upravovat a předělávat jednotlivé programy. Zločinci, kteří nerespektují práva spjaté s informatikou a licencemi. Často označování také jako „crackeři“. Nejedná se pouze o piráty, kteří porušují licenční podmínky pouze v oblasti softwaru, ale napadají i celé počítačové sítě.

Hackeři prolomují všechna možná bezpečností opatření, domlouvají se převážně pouze mezi sebou, vlastní komunitou. Vystupují pod nejrůznějšími přezdívkami, kvůli zachování jejich anonymity. Často jsou počítačově velmi gramotní a patří mezi elitu počítačových expertů. V současné době při prolomení bezpečnostních prvků vybrané vývojářské firmy vypisují odměny, aby získaly bezpečnější ochranu.

4.4.3 Warez

Produkt s licenčním ujednáním, se kterým se zachází nelegální cestou. Vytváření a šíření warezu je nelegální. Vytvářejí jej především lidé, kteří jsou označováni informačním slangem jako „počítačový piráti“. Jde o produkt, který je v rozporu s autorským zákonem. Při nedodržení ustanovení může být pirát trestně stíhán.

Průběh vytvoření warezu je velmi prostý. Vyjde program s licenčním ujednáním. Ve velké většině skupina pirátů tento program dostává rovnou z fabriky formou distribuce na CD. Pro skupinu je důležité získat produkt ještě před vydáním na trh. Program je předán do rukou hackera, který odstraní všechny bezpečností známky. Poté jej skupina rozšiřuje pomocí internetu dále mezi uživatele, nejčastěji pomocí FTP serveru a torrentů.

Jak jsem zmiňoval, warez vytvářejí a šíří především skupiny lidí. V tomto případě se už jedná o organizovanou skupinu lidí, kteří to ve valné většině dělají pro radost. Za tento trestný čin nezískávají žádný obnos peněz. Proti šíření a vytváření warezu aktivně bojuje sdružení OSA. U médií máme mnoho typu warezu, například u filmů.

Mezi nejrozšířenější patří „kinorip“, kdy jedinec natočí film přímo v sále kina a nahraje jej na server typu RapidShare. Kvalita pořízeného záznamu je velmi špatná a často se vyskytují v záznamu ostatní návštěvníci kina. Další významný typ je „telesync“, jedná se taktéž o natáčený záznam v sále kina, ale zvuk oproti kinoripu je daleko lepší, je nahráván zvlášť mikrofonem a poté synchronizován s video záznamem. Typ R5 je velmi obdobný jako telesync. Mezi dále běžné patří DVDRip a DVDR.

4.4.4 Cracking

Je metoda upravování zdrojového kódu. Slovo pochází z anglického slova crack, v českém jazyce znamená lámat. Především se jedná o odstranění jednotlivých bezpečnostních prvků. Ve většině zemí, samozřejmě i v České republice, je cracking nezákonnou činností. I přes nejrůznější techniky výrobců se stále častěji můžeme setkávat s cracknutým produktem. Základem každého crackera je program typu Disassembler. Program převádí zpět software na zdrojový kód. Nyní je mnoho typů dostupných ke stažení, mezi nejlepší se řadí Win32Dasm a IDA Pro. Tímto se člověk dostává ke zdrojovému kódu, kde bude hledat jednotlivá zabezpečení přichystané výrobcem.

Debugger neboli další nástroj hackera slouží pro prolomení ochranných prvků. Prvotní vývoj tohoto softwaru byl určen pro programátory, aby mohli nacházet chyby v systémech. Tento nástroj je tudíž samozřejmě velká pomůcka pro crackery. Jednou z největších výhod debugger je krokování instrukcí. Poté se jednoduše kontrolují hodnoty v registrech, zásobníku i paměti. Další základní funkce je breakpoint, který v určitých chvílích pozastavuje program v určitých fázích. Nachází se zde možnost zastavit program po určité instrukci.

4.4.5 Keygen

Velmi používaná metoda na překonávání bezpečnostních prvků ochrany programů. Jedná se o překonání registračního čísla. Při použití keygenu se často nainstaluje daný software jako trialová aplikace a poté se doplňuje registrační číslo pro neomezené použití. Při zadání správného platného registračního čísla se program stane zcela platným a můžeme jej používat v plném rozsahu.

Keygen představuje algoritmus, který generuje sériová čísla. Hacker, který keygen vytváří, musí nahlížet do zdrojového kódu programu a vyznat se v architektuře kódu. Nejčastěji, jak již jsem zmiňoval, se používá k těmto praktikám program dissembler. Použití vytvořeného keygenu je velmi triviální. Stačí nastavit program, pro který sériové číslo hledáme, verzi programu, kterou máme nainstalovanou a poté zmáčknout tlačítko určené pro generování. Zkopírujeme vygenerovaný kód a vložíme k ověření.

Použití keygenu není nijak trestné. Můžeme si generovat hesla, jak uznáme za vhodné. Ale jakmile heslo použijeme k prolomení bezpečnostního prvku, pak se jedná o nelegální činnost. V podstatě i většina dostupných antivirových programů, jak placených, tak programů typu freeware, nám vyhazuje hlášku o nebezpečném souboru hned při stažení keygenu.

5 Audit počítače

Audit počítače představuje zkontrolování hardwaru a softwaru, zda máme vše v pořádku a nedopouštíme se přestupků nebo trestných činů. Provádět v naplánovaných intervalech audit se mnohdy velmi vyplácí, nejčastěji ve větších firmách a korporacích. Pokud se zaměříme například na dema softwaru, můžeme mít omezené používání programů. Zde se vyskytuje mnoho auditových programů na výpomoc s kontrolou i celé sítě.

5.1 HW audit

Jedná se o detailní analýzu jednotlivých HW zařízení. Součástí je evidence, skenování hardwaru, možnosti vzdálené plochy, ale i monitoring jednotlivých událostí. Skenování poté je možné provádět ručně nebo automaticky. Lze zde nastavit jednotlivé intervaly pro skenování techniky.

Celkově hardwarový audit představuje jakéhosi správce sítě HW komponent. Slouží k inventuře jednotlivého technického vybavení. Odhaluje aktuální stav hardwaru a ukazuje na nedostatky. Samozřejmě se zde evidují i opravy a rozpočet náhrad.

Provádění auditu je velmi důležitým podkladem při opravách a renovacích hardwaru. Daná firma vidí cenový rozpočet jednotlivých oprav. Audit mnohdy nastíní, že levněji vyjde zakoupení nových komponent než oprava starších. Šetří čas a peníze velkých firem.

Monitoringem rozumíme záznamy všech informací o HW v časové ose. Monitorujeme vše od nákupu techniky přes po opravy, konfigurace, update až po vyřazení. Evidence nám následně popisuje techniku od mobilních telefonů přes tiskárny, scannery, počítače až po servery.

Výsledkem auditu je:

- kompletní evidence HW
- identifikace
- informace o users

- kontrola HW
- kontrola sítě
- možnosti rizik
- zabezpečení
- zálohování
- souhrnný report

HW audit provádí dnes mnoho firem nebo jsou dostupné programy, pomocí kterých si audit člověk může udělat sám. Máme specializované firmy na provádění jakýchkoliv PC auditů. Trh je přesycen firmami, které poskytují takovéto služby. Ve valné většině se jedná o placený software, který mnohdy není nejlevnější.

5.2 SW audit

Jedná se o detailní analýzu nainstalovaného a používaného softwaru. Stará se především o správu SW a licenční ujednání k daným programům. Jednotlivými kroky zjišťuje aktuální stav softwaru, časové omezení jednotlivých licencí programů a lze jej porovnávat s daty o zakoupení.

Hlavním úkolem softwarového auditu je legalizace veškerého softwaru v dané komunitě. Auditem ušetří firmy mnohdy nemalé částky, efektivnost používání SW na základě auditu patří k důležitým vlastnostem auditu. V neposlední řadě chrání firmu nebo korporaci podloženými daty o legalizaci všech produktů a stálou kontrolou nad technickým vybavením.

SW audit prozkoumá jednotlivé počítače, vypíše podrobný report o nainstalovaném i neinstalovaném softwaru. Ukazuje aktivnost jednotlivých licencí a zároveň upozorňuje na vypršení ostatních licencí. Lze kontrolovat počítače v rámci celé sítě. Šetří nemalé peníze při hospodaření se softwarem a pomáhá managementu.

Výhody provádění SW auditu

- kompletní přehled o SW celé společnosti či počítače
- analýzy používaného SW a možnosti návrhu efektivnější, levnější formy
- ochrana před nepříjemným trestním stíháním
- zlegalizování všech licencí a dorovnání jednotlivých nesrovnalostí se SW
- efektivnější investování do SW – multilicence ve firmách
- celkový report o stavu techniky
- ochrana jména firmy

5.2.1 Winaudit

Jeden z nejznámějších programů na softwarový audit počítače. Celkově velmi jednoduchý program na ovládání a potěší české prostředí. Jedná se o program typu freeware, který dokáže přesně zjistit mnoho podrobných informací. Zjišťuje základní informace typu název počítače, operační systém, uživatele, systémové informace, nainstalovaný software i s daty instalace, registrované knihovny, porty, systémové soubory, síťová nastavení, běžící procesy a další.

Vypisuje odborný konečný report, který lze komprimovat a odesílat e-mailem nebo jej lze uložit do databáze pro další užití. Autorem je Parmavex services. Jak již bylo zmíněno, program je distribuován pod typem licence freeware a podporuje většinu běžných operačních systémů.

5.2.2 Free PC audit 2.0

Další velmi používaný auditorský program. Dokáže analyzovat instalovaný hardware i software. Jako Winaudit vypisuje podrobné informace, které lze jednoduše exportovat do různých formátů k dalšímu použití. Jedná se, jak z názvu vyplívá, o program s licencí typu freeware. Autor programu je MIS Utilities. Free PC audit 2.0 podporuje většinu operačních systémů.

Programů na software audit je mnoho, mnohdy se setkáváme ale s programy velmi nezdařilými, pod licenčním ujednáním freeware. Winaudit a Free PC audit 2.0

jsou podle internetu a počtu stažení nejpoužívanějším freewarovým softwarem pro SW audit s licencí freeware.

Pokud se jedná o placené programy na SW audit, máme opět na výběr široké spektrum. Zde už se jen málokdy vyskytují nedostatky typu vyhledání pouze 70% programů v počítači jako například u freewarového programu Instatnt software auditor. Jsou mnohem propracovanější a přesnější, je zde široký a přesnější výběr využití pro firmy, kde se dělají audity převážně po síti.

5.3 BSA

BSA je největší aliance zabývající se informační kriminalitou na světě. Jednotliví členové zastupují BSA celkem v 80 zemích světa. Preferují používání softwaru s licenčním ujednáním legální cestou. Cílem je zvýšit gramotnost licencí, použití licencovaného software a důvěřovat ve výpočetní techniku. Členem se může stát prakticky každý spořádaný občan. Celá organizace je financována sponzory, dary a poplatky účastníků. Bojují tímto i proti korupci a podplácení.

Z výzkumů BSA vyplívá, že v České republice jsou stále obrovské cifry, které značí újmu výrobcům softwaru s licenčním ujednáním. Z prováděných výzkumů je patrné, že nejvíce firem s počtem zaměstnanců od pěti do stovky, se dopouští porušování autorského práva. Naopak nejlépe jsou na tom firmy, korporace a instituce s více než 250 zaměstnanci. Tyto firmy mají již ve velké míře prostředky na pořizování auditů, jak hardwaru, tak softwaru. V jejich měřítku to přináší mnohdy několika cifrové šetření prostředků při provádění auditů, a samozřejmě mají komplexní přehled o aktuálním dění na trhu a výjimečně se dopouštějí porušování autorského zákona v oblasti informační kriminality.

Nejčastěji zneužívané programy jsou od společnosti Microsoft, Adobe, Symantec, Corel, Autodesk a jiné. Dle statistik z roku 2010 se v Česku užívalo až 40% nelegálního softwaru, což činilo ztráty až ke třem miliardám korun.

BSA vytváří různé statistiky a fakta, dle kterých se snaží zasáhnout do boje proti informační kriminalitě. Sama The Software Alliance jde příkladem a má za cíl nastolit řád ve všech zemích svým účinkováním.

5.3.1 Postupy vyhledávání BSA

Prvním krokem je vždy vyhledání daného hříšníka, který používá nelegálně nějaký software. Organizace je postavená na jednotlivých členech, kteří shromažďují data a podklady v konkrétní zemi. Mají zastoupení po celé Evropě, tudíž dodržují postupy a pracují v teamu. Jednotlivé tipy o nelegální činnosti získávají od běžných obyvatel dané země. Vyhlašují různé soutěže a slibují všemožné odměny. V České republice bohužel začátkem roku 2001 aliance zkazila reputaci příliš agresivními kampaněmi proti počítačovému pirátství. Aliance vedla mnoho zásahů proti údajným pirátům, samozřejmě legální cestou. Podávala mnoho podmětů Policii ČR o údajné informační kriminalitě. Bohužel mnoho těchto podmětů nebylo pravdivých a docházelo k pošramocení celé skupiny bojující proti kriminalitě.

Vyvrcholilo to rokem 2001, kdy došlo Policií ČR k zásahu v malém podnikatelském objektu. Zde se měl používat software nelegální cestou. Bohužel se zde nic nenašlo a ne příliš líbivý video záznam ze zásahu obletěl svět. Je možné ho shlédnout na serveru youtube.com i dnes. Nejhorší na těchto situacích bylo zabavení veškeré výpočetní techniky firmě a to i s kompletním účetnictvím. Proto poté docházelo ke zdlouhavým procesům vymáhání odškodného za ušlý zisk a žádaly se vysoké částky o náhradu celé napáchané škody.

Ze získaných zkušeností se aliance poučila a před urgováním Policie ČR, provedením prohlídek a zabavováním techniky a podkladů, začala rozesílat oznámení malým firmám. Jednalo se o fakt, že BSA dostala podmět o nelegálním používání softwaru ve firmě a než aby hned zahájili celý proces s Policií ČR, stačilo nejdříve zaslat firmě dopis, že mají informaci o užívání SW bez licenčního ujednání nebo programy typu freeware a upozornit firmu na to. Firmě nabídnout možnost vyplnit prohlášení o typu užívaného SW.

Následně zpracovává BSA různé studie o pirátství v České republice, které mají opět mnoho kritiky. Vycházejí totiž z nepodložených faktů a tak nutno podotknout, že ve skutečnosti to může být jinak. Rozhodnutí posledních let aliance zní jasně, zaměřit se na malé a střední firmy, jelikož velké firmy mají dnes velmi dobré SW postupy a zpravidla zde nedochází k obcházení licenčního ujednání a tvorbě warezu.

V této době do České republiky přichází novinky používané ve světě již několik let. Dříve lidé podávali alianci ve valné většině anonymně údaje o porušování autorského práva, neboť nechtěli přijít o práci a zbytečně na sebe ukazovat. Bylo to velmi složité i pro udávání podmětů k domovním prohlídkám, kontrolám atd. Policie mnohdy nemohla alianci vyhovět. Projekt nazvali program „Texaských rangerů“. BSA si slibuje od tohoto programu mnoho výhod a nárůst boje proti informační kriminalitě z pohledů zaměstnanců firem. Jednoduše řečeno, člověk, který ví o nelegálním používání softwaru, může nahlásit alianci tuto činnost. Aby se tento jedinec neschovával za anonymitou, bude mu nabízena deseti procentní výše z odškodněného. Zpravidla se to bude vyplácet „lovcům pirátů“, kteří upozorní na větší firmy s více nelegálními softwary. Odměna je stanovena kvůli motivaci a ztrátě příjmů jedince.

Na oficiálních stránkách aliance BSA si může každý zdarma stáhnout software na audit počítače od společnosti Attest Systems Inc. Tato firma spolupracuje s aliancí a bojuje tím proti pirátství v osmdesáti zemích světa.

6 Forenzní praxe informační kriminality

Forenzní analýza je pojem pro hloubkovou analýzu a vyšetřování, jehož účelem je objektivně určit a zdokumentovat viníky, důvody, průběh a důsledky nějakého bezpečnostního incidentu nebo porušení práva státu či pravidel organizace. Zjednodušeně řečeno, forenzní analýza vyšetřuje přestupek či trestný čin - prokazuje kdo, jak a kdy něco zavinil. Často souvisí se soudním dokazováním, zejména v trestních záležitostech. Zahrnuje využití širokého spektra vyšetřovacích technologií, postupů a metod. Forenzní specialisté shromažďují různé typy informací, pracují jak s elektronickými zařízeními, tak klasickým způsobem s informacemi na papíru. Forenzní analýza vychází z oboru Forenzika (Forenzní věda). *(Forenzní analýza, 2013)*

6.1 Forenzní analýza

Forenzní analýza - tento termín se nepoužívá pouze v oboru informatiky, ale například i v oboru psychologie, účetnictví a managementu. Provádění forenzní analýzy má své důležité opodstatnění. Jedná se o nezbytný podklad při vyšetřování. Používá se samozřejmě v kriminalistice, využití má převážně pro Policii ČR, ale využívají ji také různé organizace, ve kterých se jedná o interní vyšetřování v rámci organizace. Odborně se tento termín ve velkých organizacích nazývá forenzní metody vyšetřování.

Nejčastěji provádějí forenzní analýzu vyšetřovatelé. U velkých organizací se ve valné většině najímají externí vyšetřovatelé, aby nedošlo ke střetu zájmů a ovlivnění celkové analýzy. U Policie ČR tuto funkci zastávají jednotlivá oddělení. Spjaté s informační kriminalitou a daným tématem jsou na území České republiky dvě důležitá oddělení zabývající se porušováním autorského zákona licenčního ujednání softwaru a porušováním práv u médií.

Forenzní věda (nebo zkráceně forenzika, forensics) je vědní obor, který se zabývá vyšetřováním, získáváním a (soudním) dokazováním nějakého bezpečnostního incidentu nebo porušení práva státu či pravidel organizace. Forenzní věda vytváří a zlepšuje postupy vedoucí k prokázání identity osob, pravosti dat, pravosti listin,

identifikace zbraní, chemikálií a podobně. Využití forenzních věd a postupů při vyšetřování se nazývá forenzní analýza. *(Forenzní analýza, 2013)*

Forenzní analýza disků je tedy věda, která spojuje mnoho témat. K pochopení je potřeba alespoň základní znalosti hardwaru, operačních systémů, sítí, softwaru a mnoho dalšího. Bez příslušných zkušeností můžeme analýzu provádět neodborně a poté znehodnotit celý výsledek.

6.2 Postup při zásahu

Obor informatiky je v dnešní době velmi rozsáhlý. Z tohoto důvodu se doporučuje mít prvotní přehled o zkoumaném objektu. Základními aspekty jsou rozloha a umístění zkoumaného objektu, znalost personálu v oboru informatiky, základní hardwarové řešení objektu a používání programového vybavení.

Díky těmto základním informacím se technikovi mnohem lépe pracuje a dokáže se připravit na odborné zabavení techniky. Připravenost se později odráží i na další prováděné forenzní analýze a samozřejmě na výsledném reportu.

Před samotným zabezpečením techniky je velmi důležité prostředí při zásahu. Neměl by zde bránit ve výkonu práce personál objektu. Data jsou velmi snadno zničena, proto je velmi důležitá koncentrace a přesný zásah dle standardů Policie ČR. Samotné zajištění techniky vykonávají speciálně proškolení technici, kteří mají dostatečnou kvalifikaci nebo jsou pod dohledem odborníka. Nejčastěji zasahují techničtí kriminalisté z útvaru Policie ČR jménem OKTE (oddělení kriminalistické techniky), kriminalistického ústavu nebo civilní znalec s příslušnou kvalifikací.

Platí, že nesmí jakýkoliv personál ani policista neproškolený na výpočetní techniku manipulovat při zásahu domovní prohlídky s technikou. Toto zabezpečení je kvůli možné hrozbě ztracení dat a údajů. U soudu by bylo velmi jednoduché zamítnout důkaz nebo techniku z důvodu neodborné manipulace s technikou a upravení zabavených dat.

Při zabavování techniky se můžeme setkat se zabezpečením proti manipulaci neoprávněnou osobou. Vyskytují se i různé softwarové defragmenty, které znehodnotí data a výsledkem je zbytečná domovní prohlídka. Proto jsou nezbytní

odborníci na zabavení techniky a pro následné možné vytváření analýz k trestnímu stíhání.

Zabavované věci pro tvorbu forenzní analýzy v oblasti informatiky:

Počítače, servery, notebooky a jiné, u rozsáhlejších objektů se zabavují pouze pevné disky z PC. Pokud by bránily zabavené věci výkonu práce, docházelo by k ušlému zisku, se provádí v těchto případech takzvané image disků.

Datová média, tím rozumíme přídavné pevné disky, CD ROM, DVD ROM, diskety a jiné.

Dokumenty, vztahující se k informační kriminalitě nebo k zabavené technice.

Prvotně je provedena fotodokumentace veškeré zabavované techniky. Poté je velmi důležité rozhodnutí, zda techniku vypnout, odpojit a odvést nebo vytvořit zálohu veškerých dat, jako například dočasných souborů a jiné. Vše samozřejmě záleží na objektu, využívání techniky a nebránění výkonu práce.

Technika je samozřejmě vlastnictvím majitele, tudíž se na ní vztahují vlastnická práva. Je nezbytné při zabavení techniky ji zdokumentovat, zapečetit a zabalit, aby nedošlo k poškození důkazů i techniky.

V neposlední řadě patří mezi dokumentaci hesla a oprávnění. Zabavují se při domovní prohlídce taktéž. Údajný pachatel nesmí narušovat průběh zásahu a měl by spolupracovat s vyšetřovateli a techniky.

Postupem času jde technika velmi rychle kupředu. Technici se nesetkávají už jen s počítači, servery a základním vybavením předešlých let. Dnes jsou velmi populární mobilní telefony typu smartfoun, tablety, PDA a různá zařízení připojená na internet. U tohoto typu elektroniky se zpravidla musí zajistit odpojení od sítě a internetu, aby nedošlo k dálkovému smazání nebo porušení dat.

Metodika práce, postupy při zásahu domovní prohlídky, všechny tyto dokumenty jsou v České republice vedeny jako interní směrnice příslušného orgánu. Na internetu je mnoho technické dokumentace, dle které možná postupuje policie při zásahu, ale žádný z těchto dokumentů nemusí být směrodatný. S pohledem na

extrémně rychlý vývoj techniky jsou dokumenty jako metodika a postupy práce rychle nahrazovány a zdokonalovány.

6.2.1 Domovní prohlídka

Domovní prohlídku může příslušný orgán vykonat pouze tehdy, pokud je důvodné podezření na páchání informační kriminality. K vykonání potřebuje orgán „příkaz k domovní prohlídce“ vystavený soudcem. U domovní prohlídky má právo být zletilý člen firmy, domácnosti. Ve výjimečných případech jsou přítomni i další pozorovatelé, například u právní firmy bude přítomen člen zástupce advokátní komory.

6.2.2 OKTE

Odbor kriminalistické techniky a expertíz. Historicky první akreditované znalecké pracoviště Police v České republice.

Své služby poskytuje především orgánům činným v trestním řízení, a to v oblasti zajišťování důležitých důkazů pro soudní líčení. Odbor zpracovává znalecké posudky v oblasti klasických (daktyloskopie, mechanoskopie atd.), ale i moderních forenzních disciplín jako je genetika, chemie či počítačová expertíza. Vysoká kvalita práce je proto na tomto pracovišti nutností. V březnu roku 2007 se OKTE PČR Správy Východočeského kraje Hradec Králové stal historicky prvním policejním akreditovaným pracovištěm v ČR. Vlastnictvím osvědčení o akreditaci prokazuje toto pracoviště špičkový systém práce a maximální věrohodnost a objektivitu svých znaleckých posudků. *(ČR, 2010)*

6.3 Postup zkoumání techniky

Zabezpečená technika je zapečetěná a zabalená odvezena z místa zásahu do příslušné laboratoře specifického orgánu. Než se technika zprovozní a začne se provádět forenzní analýza, vše se kontroluje a dokumentuje, aby nedošlo k pochybení.

Jednotlivé kroky před začátkem forenzní analýzy:

Zkoumání neporušenosti obalů, v kterých je technika převážena a kontrola pečetí.

Kontrola a dokumentace jednotlivé techniky, porušenost, identifikace výrobních čísel, příslušná kabeláž a vše s tímto spjaté.

Dochází k rozebrání a dokumentaci techniky (např. case počítače[1]), kontrolují se veškeré komponenty uvnitř a jejich viditelné poškození.

V určitých typech případů se demontují některé komponenty, nejčastěji pevné disky, které se zdokumentují, zapisují se sériová čísla, nastavení, poškození a jiné.

Dokumentace je prvním krokem analýzy, vyšetřovatelé z ní vycházejí k podrobnému zkoumání. Zároveň slouží jako důkaz o stavu techniky před důkladnějším zkoumáním.

6.3.1 Zajištění dat

Hlavním cílem zajištění dat je vytvoření přesné kopie zkoumaného disku. Nejdůležitější při této operaci je nepoškodit data na zkoumaném médiu a zachovat tak průkaznost důkazu. Tento krok vyžaduje několik nástrojů a mnoho času dle velikosti zkoumaného objektu.

Vytvoření image[2] disku lze provést několika způsoby. Novější operační systémy mají zabudované nástroje pro vytvoření zálohy, ale touto zálohou nelze provést forenzní analýzu. Na internetu lze nalézt mnoho softwaru na vytvoření image disku, které jsou pod licencí např. freeware.

Nejčastějším nástrojem na vytvoření obrazu disku, který provádějí znalci nebo policie, je nabootování operačního systému. Operační systém můžeme mít nainstalovaný přímo na počítači nebo jej pouštět z live distribuce[3]. Budu popisovat postup s využitím live distribuce operačního systému Linux. K provedení nabootování potřebujeme:

Disk s větší kapacitou, než je zkoumaný disk.

Operační systém pro forenzní zkoumání. Jak jsem již zmínil, nejčastěji se používá operační systém Linux spouštěný jako „live distribuce“. Znamená to nabootování

[1] Case – počítačová skříň
[2] Image – obraz disku, úplná kopie
[3] Live distribuce – operační systém pouštěný z externího disku nebo média

systému z přídavného zařízení, z cílového disku nebo optického média, který nepřipojuje pevné disky při startu celého počítače.

Pokud bychom vytvářeli bitovou kopii příslušným softwarem, budeme potřebovat program a disk, který je kapacitou větší než zkoumaný disk.

Při nabootování systému a následném jeho spuštění se připojí zkoumaný disk a provede se kontrola dat součtem.

6.3.2 Hashovací funkce

Funkce zajišťující prokazatelnost zajištěné techniky. Používá se vždy ještě před provedením bitové kopie. Slouží jako podklad pro soud, že nebylo jakkoliv manipulováno s daty na zabaveném disku. Data jsou velmi křehká a znehodnocení důkazů by vedlo k neprokazatelnému důkazu.

Pomocí hashovací funkce vytvoříme soubor jménem logs.md5, ve kterém je kontrolní součet celého zkoumaného disku a musí se shodovat se součtem provedeným na konci analýzy. V praxi se kontrolní součet vytiskne a podepíší se pod dokument technik a příslušná osoba.

Poté lze snadno provést kopii disku na příslušný zkoumaný disk.

Image disku je celková kopie zkoumaného disku, včetně „prázdného prostoru“. Nazývá se také obraz disku. Je to posloupnost jednotlivých bitů. Kopírování probíhá funkcí bit po bitu. Nikdy se nevytratí jakýkoliv bit, který byl na originálu.

6.3.3 Používané systémy pro forenzní analýzu

Příslušný orgán POLICIE ČR zabývající se forenzní analýzou využívá několik forenzních systémů. Shrnutí nejpoužívanějších z nich:

Deft je linuxový operační systém vytvořený přímo pro forenzní analýzu. Najdeme zde mnoho nástrojů usnadňujících práci. Byl vytvořen především pro zkoumání celého počítače. Volně stažitelný operační systém stejně jako všechny produkty Linuxu. Nabízí funkci připojení disků pouze pro čtení.

Back Track 5 je velmi populární linuxová aplikace na provádění auditů nebo analýzy bezpečnostních průniků. Určená především pro bezpečnostní analytiky. V novějších verzích podporuje funkci připojení disků pouze pro čtení.

Caine - Computer Aided Investigative Enviroment je nástroj primárně určený pro vyšetřovatele. Opět má velmi dobře řešené nástroje, zejména pro připojení disků.

6.3.4 Postup získávání dat

Oddělení Policie ČR zabývající se informační kriminalitou využívá nejčastěji software EnCase a Forensic Toolkit 5. Jedná se o vyspělé programy na odhalování informační kriminality. Pomáhají k dopadení pachatelů, kteří se dopustili všech typů trestných činů za pomocí výpočetní techniky. Zobrazují data v různých formátech zobrazení, poskytují kompletní náhled do registrů, vytvářejí grafy z nalezených dat a rychlé vyhledávání mezi daty. Funkce EID – Explicitní Image Detectio, funkce automatické identifikace pornografických obrázků.

Ve vztahu k licenčním ujednáním software dokáže porovnávat hash klíče s klíči uloženými v externí databázi, dle které lze dokázat cracknutí programu, tudíž porušení autorského práva.

Hash klíč je jednoznačné identifikační číslo softwaru. Pokud pirát obejde bezpečnostní prvky programu nejčastěji v samotném kódu, změní velikost souboru. Byť se jedná o navýšení nepatrné velikosti kódu, hash klíč bude rozdílný. Lze pak jednoznačně určit porušení licenčních podmínek, pokud se jedná o placený software nebo jinak chráněný.

Tato metoda je velmi zdlouhavá, ne vždy se hash klíče dají najít a program by musel aktualizovat databázi všech hash klíčů na světě, zároveň by všechny musely být shromážděny v jedné databázi.

Programy EnCase a Forensic Toolkit 5 jsou především určeny pro oblasti informační kriminality na nelegální přechovávání a stahování hudby a filmů, vyhledávání dětské pornografie a vyhledávání důkazů ve výpočetní technice o páchání trestného činu. Nejsou primárně určeny na vyhledávání nelegálně instalovaného, používaného softwaru.

Informace o nalezených programech na disku počítače se získávají vyhledáváním ve složkách, prozkoumáváním celého počítače. Stále nejúčinnější metoda získání dat o SW je po připojení na unixový operační systém Linux, kde po nabootování zkoumaného disku pomocí příkazů lze zjistit nejvíce informací o softwaru nacházejícím se na disku.

7 Praktická část - navržený postup forenzní analýzy

Cílem postupu je zajištění kompletního výpisu všech programů a audio, video souborů a dosáhnutí výsledného auditu zkoumaného počítače za použití pouze bitové kopie. Důležitým požadavkem je zkoumání disku pouze z image. Výsledný report bude vyexportován do formátu CSV, na kterém budou patrné všechny zkoumané informace.

7.1 Použité nástroje

- Operační systém Linux verze DEFT, live distribuce[4]
- Unixový nástroj md5sum[5]
- Externí disk
- Vytvořený skript

7.2 Příprava systému a disku

Prvním krokem je získání operačního systému Linux verze DEFT, který je poskytován zcela zdarma. Vytvořením live CD nebo disku, kde bude připravený systém pro spuštění na daném počítači. Pro rychlou přípravu může pomoci mnoho aplikací pro rychlé vytvoření live verze OS DEFT.

Potřebujeme externí disk větší než zkoumaný disk pro vytvoření a uložení image disku. Externí disk by měl být nejlépe prázdný nebo alespoň by měl obsahovat více volného místa než zkoumaný disk. Nejlépe je, když bude rozdělený na více oddílů, kde využijeme celý jeden oddíl. Naformátovaný dle výchozího nastavení na NTFS[6] nebo FAT 32.[7]

[4] Linux, DEFT - operační systém, vytvořený přímo pro forenzní analýzu
[5] md5sum – nástroj pro vytvoření kontrolního součtu
[6] NTFS – souborový systém
[7] FAT 32 – souborový systém

7.3 Vytvoření image

Pro vytvoření image blokového zařízení potřebujeme znát jeho identifikátor. Ten můžeme zjistit příkazem

```
fdisk -l
```

Výstup tohoto příkazu může vypadat například následovně:

```
Disk /dev/sda: 232.9 GiB, 250059350016 bytes, 488397168 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x77d5bb87

Device     Boot     Start       End    Blocks  Id System
/dev/sda1              63 102402047  51200992+ 83 Linux
/dev/sda2       102402048 381900799 139749376  83 Linux
/dev/sda3 *     381900800 382310399    204800  af HFS / HFS+
/dev/sda4       382310400 488394751  53042176  af HFS / HFS+


Disk /dev/mmcblk0: 7.5 GiB, 8032092160 bytes, 15687680 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00000000

Device         Boot Start       End  Blocks  Id System
/dev/mmcblk0p1       8192  15687679 7839744   b W95 FAT32


Disk /dev/sde: 931.5 GiB, 1000204886016 bytes, 1953525168
  sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x0007e9f5

Device     Boot Start        End    Blocks  Id System
/dev/sde1       2048 1953523711 976760832  83 Linux
```

Na tomto výpisu vidíme, že k počítači jsou připojeny tři disky. Prvním diskem je disk identifikovaný jako */dev/sda*, druhy */dev/mmcblk0* a třetí */dev/sde*. Řekněme, že se budeme zabývat diskem prvním, tedy */dev/sda*. Vidíme, že tento disk je rozdělen na čtyři oddíly identifikované jako */dev/sda1* až */dev/sda4*.

7.3.1 Vytvoření image celého disku

Chceme-li vytvořit image celého disku */dev/sda* a výslednou image uložit do souboru image v aktuálním pracovním adresáři, použijeme příkaz

```
1   dd if=/dev/sda of=image
2
```

7.3.2 Vytvoření image jednoho oddílu

Řekněme, že nás z celého disku */dev/sda* zajímá pouze oddíl */dev/sda1*. Bylo by zbytečné kvůli jednomu oddílu kopírovat celý disk. Bitovou kopii oddílu */dev/sda1* vytvoříme příkazem

```
1   dd if=/dev/sda1 of=image
2
```

7.3.3 Připojení image

Soubory Linuxového souborového systému jsou uchovávané v jedné stromové struktuře a začínají od kořenového (root) adresáře /. Soubory v rámci této stromové struktury mohou být fyzicky uloženy na různých zařízeních.

K tomu, abychom mohli v Linuxu připojit blokové zařízení do stromu souborového systému, se používá příkaz *mount*. Základní syntaxe je následující:

```
1   mount -t type device dir
2
```

Tento příkaz připojí zařízení device se souborovým systémem type do adresáře *dir*. Pokud chceme připojit oddíl nějakého fyzického disku, je device typicky */dev/sdxn*, kde x ∈ 2 {a,b,…..z,aa,….} a *n* je číslo připojovaného oddílu. Oddíly jsou

číslované od jedné. Seznam dostupných zařízen a jejich oddílů si můžeme nechat vypsat příkazem *fdisk -l*.

Úkolem našeho skriptu je připojit image. Jelikož *mount* pracuje s blokovými zařízeními, je nejprve nutné vytvořit virtuální blokové zařízení.

Virtuální blokové zařízení, nebo také loop zařízení, je zařízení, které zpřístupňuje soubor jako blokové zařízení. Virtuální blokové zařízení nám tedy umožní se souborem image pracovat tak, jako by to byl fyzický disk připojený k našemu počítači.

7.3.4 Připojení image celého disku

Pokud náš image obsahuje více diskových oddílů, je nutné vytvořit virtuální zařízení ručně. Příkazem *fdisk -lu image* si můžeme vypsat seznam oddílů z image disku. Výstup může vypadat například následovně:

```
1  Disk /media/bckp/sda: 18 GiB, 19327352832 bytes, 37748736
     sectors
2  Units: sectors of 1 * 512 = 512 bytes
3  Sector size (logical/physical): 512 bytes / 512 bytes
4  I/O size (minimum/optimal): 512 bytes / 512 bytes
5  Disklabel type: dos
6  Disk identifier: 0x931a7fc7
7
8  Device           Boot     Start       End   Blocks  Id System
9  /media/bckp/sda1 *         2048    206847   102400   7 HPFS/NTFS
     /exFAT
10 /media/bckp/sda2         206848  37746687 18769920   7 HPFS/NTFS
     /exFAT
11
```

Řekněme, že chceme analyzovat oddíl */dev/sda2*. Abychom mohli vytvořit virtuální blokové zařízení reprezentující tento oddíl, musíme si nejprve spočítat offset (počáteční bajt oddílu). Z výpisu výše vidíme, že náš oddíl začíná sektorem číslo 206848, tento sektor si označíme jako *start*. Dále ve výpisu vidíme, že velikost sektoru je 512 bajtu, velikost si označíme jako *ssize*. Z těchto údajů již můžeme vypočítat offset:

$$offset = start * ssize$$

V našem případě bude offset tedy 206848 512, což je 105906176. S vypočteným offsetem již můžeme vytvořit virtuální blokové zařízení příkazem

```
losetup -o offset /dev/loop0 image
```

V našem případě

```
losetup -o 105906176 /dev/loop0 image
```

Tento příkaz vytvoří virtuální blokové zařízení z oddílu, který začíná na daném offsetu image souboru image. Toto zařízení bude dostupné přes soubor */dev/loop0*. Pokud v */dev* žádný loop zařízení nemáme, pravděpodobně máme novější jádro. Od určité verze jádra je potřeba modul loop ručně zavést. To můžeme provést například příkazem

```
modprobe loop
```

Když máme vytvořené virtuální blokové zařízení, můžeme ho vytvořit příkazem

```
mount /dev/loop0 dir
```

kde *dir* je cílový adresář.

Po ukončení práce s image je vhodné image odpojit příkazem

```
umount dir
```

Virtuálních zařízení máme k dispozici pouze omezený počet. Pokud tedy již virtuální blokové zařízení nepotřebujeme používat, je slušné od něj odpojit soubor image, aby ho mohli používat ostatní uživatelé. Toto provedeme příkazem

```
losetup -d /dev/loop0
```

7.3.5 Připojení image jednoho oddílu disku

Ruční vytváření virtuálního blokového zařízení není nutné v případě, že připojujeme pouze image jednoho oddílu disku { v takovém případě můžeme použít parametr *-o loop* a *mount* si virtuální blokové zařízení vytvoří sám. Máme-li tedy soubor s image pojmenovaný *image* a chceme ho připojit do adresáře *dir*, stačí nám použít příkaz

```
mount image dir -o loop
```

Pokud připojenou image už nepotřebujeme používat, je opět vhodné ji odpojit z adresáře *dir* příkazem

```
umount dir
```

7.4 Vyhledávání souborů

Úkolem skriptu má být vyhledat soubory s příponami exe a com. K tomuto účelu se dá využít unixový příkaz *find*. Find umožnuje rekurzivně prohledávat zadaný adresář a dovoluje nám nastavit celou řadu parametrů a vyhledávacích kritérií. Pro naše účely si vystačíme s parametrem *-name*, který udává název vyhledávaného souboru. Parametr *-name* může obsahovat zástupné znaky. Pokud chceme vyhledat například všechny exe soubory v adresáři *dir*, použijeme příkaz

```
find dir -name "*.exe"
```

7.5 Funkce skriptu

Skript v současné dobé umí vyhledávat exe a com soubory v zadané image. Vstupem skriptu je soubor s image celého disku.

Po spuštění skriptu je nám vypsán seznam diskových oddílů, který obsahuje vstupní image. Zadáním čísla oddílu provedeme jeho výběr. Skript si spočítá offset, vytvoří si virtuální blokové zařízení a disk připojí do adresáře mount *-%y-%m-%d-%H-%m-%S*. Z důvodu předcházení kolizím v názvech adresářů se v názvu vyskytuje aktuální datum a čas. Do tohoto vytvořeného adresáře je následně připojeno virtuální blokové zařízení. Pokud vše proběhne v pořádku, najdou se zadané soubory a jejich cesty se zapíší do výstupního souboru. Po dokončení vyhledávání je virtuální blokové zařízení odpojeno z adresáře, tento dočasný adresář je smazán a virtuální blokové zařízení je uvolněno.

7.5.1 Parametry skriptu

Pokud skript spustíme bez parametrů, vypíše nám základní použití

```
1    Usage: ./exefinder.sh -i image_file -e <true|false> -c <true|
     false> -o output_file
2
```

Parametr *-i* specifikuje vstupní soubor s image disku. Parametrem *-e* se vypne/zapne vyhledávání exe soubor. Parametrem *-c* se vypne/zapne vyhledávání com souborů. Parametr -o udává výstupní soubor, ve kterém bude uložen seznam nalezených souborů.

7.6 Skript pro mediální soubory

Skript lze využít i pro vyhledávání mediálních souborů z důvodu nalezení licenčních podmínek i u takovýchto druhů souborů. Upravil jsem stávající skript do podoby pro vyhledávání mediálních souborů. Mění se pouze zadání parametrů, které chceme, aby skript vyhledal. Pokud opět skript pustíme bez parametrů, vypíše nám nápovědu pro použití. Spuštění skriptu je stejné jako při vyhledávání souborů s koncovkami exe a com. Pouze lze přidat parametry pro vyhledání například koncovky souboru avi a mp3. Dále se zeptá při nalezení několika oddílů, jaký oddíl prohledat. Funkčnost

skriptu je velmi podobná a ovládání je téměř totožné. Možnost rozšíření pro vyhledávání více typů koncovek souborů je velmi triviální, stačí pouze dopsat do skriptu další typy koncovek, jaké bychom chtěli vyhledat.

8 Návod na použití skriptu

8.1 Vytvoření image

Abychom mohli analyzovat obsah image, musíme nejprve image vytvořit. Návod na vytvoření image disku viz sekce Vytvoření image. V pokračování návodu předpokládáme, že máme v aktuálním pracovním adresáři soubor s image celého disku s názvem *image*.

Řekněme, že chceme najít všechny exe a com soubory na druhém oddílu a jejich seznam uložit do souboru *out*. Skript tedy spustíme následovně

```
sudo ./exefinder.sh -i image -e true -c true -o out
```

Při spuštění skriptu, je nám vypsán seznam diskových oddílů, které image obsahuje

```
Please select target partition:
==============================


1. image1 2048 HPFS/NTFS/exFAT
2. image2 206848 HPFS/NTFS/exFAT
```

Oddíl vybereme zadáním jeho čísla { v našem případě tedy zadáme číslo 2 a potvrdíme klávesou enter. Nyní skript vyhledá všechny odpovídající soubory a zapíše je do souboru *out*.

8.2 Postup řešení při hledání softwaru

Vytvořil jsem postup pomocí skriptu pro vyhledávání softwaru na připojeném disku s bitovou kopií. Zde ukážu funkčnost skriptu a popíši důležité kroky.

```
#!/bin/bash

LOOP_DEVICE=loop5
```

Příkaz pro zadání vstupních parametrů pro vyhledávání v image disku.

```
usage ()
{
  echo "Usage: $0 -i image_file -e <true|false> -c <true|false> -o
output_file" >&2
  exit 1
}
```

V následujícím příkazu, dochází k analýze argumentů.

```
# parse arguments

while getopts ":i:e:c:o:" op; do
  case "${op}" in
    i)
      image=${OPTARG}
      ;;
    e)
      exe=${OPTARG}
      ;;
    c)
      com=${OPTARG}
      ;;
    o)
      out=${OPTARG}
      ;;
    *)
      usage
      ;;
  esac
done
shift $((OPTIND-1))

if [ -z "${image}" ] || [ -z "${exe}" ] || [ -z "${com}" ] || [ -z "${out}"
]; then
  usage
fi

if [ $exe != "true" ] && [ $exe != "false" ]; then
  usage
fi

if [ $com != "true" ] && [ $com != "false" ]; then
  usage
fi

if [ $com == "false" ] && [ $exe == "false" ]; then
  exit 0
fi
```

Zde je ošetřen výběr diskového oddílu.

```
# select partition

SECTOR_SIZE=`fdisk -lu "$image" | grep "Sector size" | cut -d'/' -f2 | cut
-d' ' -f2`
```

```
PARTITIONS=`fdisk -lu image | cut -c-$(( \`fdisk -lu image | grep Start |
grep -b -o Start | cut -d: -f1\` + 5 )) | grep Device -A20 | tail -n +2`
```

Příkazy pro zadání vstupních dat o jednotlivých oddílech. Následně dojde k prozkoumání zadaného oddílu.

```
echo "Please select target partition:"
echo "==============================="
echo "$PARTITIONS"

read PARTITION_NUMBER

if ! [ "$PARTITION_NUMBER" -eq "$PARTITION_NUMBER" ] 2> /dev/null; then
  echo "error: Not a number" >&2
  exit 1
fi

if [ $PARTITION_NUMBER -gt `echo "$PARTITIONS" | wc -l` ] || [
$PARTITION_NUMBER -le 0 ]; then
  echo "error: Invalid number" >&2
  exit 1
fi

PARTITION_START=`echo "$PARTITIONS" | head -n$PARTITION_NUMBER | tail -n1 |
awk '{print $2}'`

OFFSET=$(($SECTOR_SIZE * $PARTITION_START))
```

Následujícími příkazy dochází k vytvoření adresáře, nazvaného aktuálním datem. Dochází k namountování. Více viz kapitola 7.5 Funkce skriptu.

```
# mount

MOUNT_DIR=`date +"mount-%y-%m-%d_%H-%m-%S"`
mkdir $MOUNT_DIR
if [ $? -eq 1 ]; then
  echo "error: could not create direcotry $MOUNT_DIR" >&2
  exit 1
fi


if [ `mount | grep $LOOP_DEVICE | wc -l` -gt 0 ]; then
  echo "warn: $LOOP_DEVICE already mounted"
  echo "umount?"

  read umount

  if [ "$umount" == "y" ]; then
    umount -d /dev/$LOOP_DEVICE 2> /dev/null
  else
    exit 1
```

```
  fi
fi
losetup -d /dev/$LOOP_DEVICE 2> /dev/null


losetup -o $OFFSET /dev/$LOOP_DEVICE $image
if [ $? -eq 1 ]; then
  echo "error: could not setup loop device" >&2
  exit 1
fi

sleep 1
mount /dev/$LOOP_DEVICE $MOUNT_DIR
if [ $? -eq 1 ]; then
  echo "error: could not mount /dev/loop to $MOUNT_DIR" >&2
  exit 1
fi
```

Tato část skriptu je jedna z nejdůležitějších. Dochází zde k nalezení odpovídajících souborů, které hledáme.

```
# find corresponding files

rm $out

if [ $exe == "true" ]; then
  find $MOUNT_DIR -name "*.exe" >> "$out"
  if [ $? -eq 1 ]; then
    echo "error: could not write to file $out" >&2
    exit 1
  fi
fi

if [ $com == "true" ]; then
  find $MOUNT_DIR -name "*.com" >> "$out"
  if [ $? -eq 1 ]; then
    echo "error: could not write to file $out" >&2
    exit 1
  fi
fi

sleep 1
```

Následující oddíl skriptu, zajišťuje odmountování.

```
# umount

umount $MOUNT_DIR
if [ $? -eq 1 ]; then
  echo "error: could not umount $MOUNT_DIR" >&2
  exit 1
fi
```

```
losetup -d /dev/$LOOP_DEVICE
if [ $? -eq 1 ]; then
  echo "error: could not detach /dev/$LOOP_DEVICE" >&2
  exit 1
fi

rmdir $MOUNT_DIR
```

8.3 Postup při hledání médií

Vytvořený skript na vyhledávání mediálních souborů je velmi obdobný. Jednoduchým přidáním více parametrů může skript vyhledávat více typů souborů. Dokládám jej v příloze k bakalářské práci.

8.4 Možnosti rozšíření

Před současným řešením skriptu se dá soubor snadno skrýt pouhým změněním jeho přípony, bylo by tedy vhodné implementovat nějaké chytřejší vyhledání na základě obsahu souboru. Toto by se dalo řešit například tak, že bychom nehledali soubory podle jejich jména, ale použili bychom akci *exec* příkazu find a pro každý soubor v image bychom spustili příkaz *file*, abychom zjistili typ souboru i u přejmenovaných souborů. Toto řešení by tedy pravděpodobně našlo více souborů, na druhou stranu by však bylo znatelně pomalejší, protože by se na každý soubor v image musel pouštět příkaz *find*. Tato možnost by tedy měla být pouze volitelná, aby uživatel mohl provést rychlé vyhledávání stejně, jak je to možné v aktuální verzi skriptu.

Skript očekává podle zadání, že na vstupu bude image celého disku. Nicméně vzhledem k tomu, že ne vždy nás zajímají soubory z celého disku, by bylo užitečné doplnit také podporu i pro image jednotlivých oddílů.

9 Výsledky průzkumu

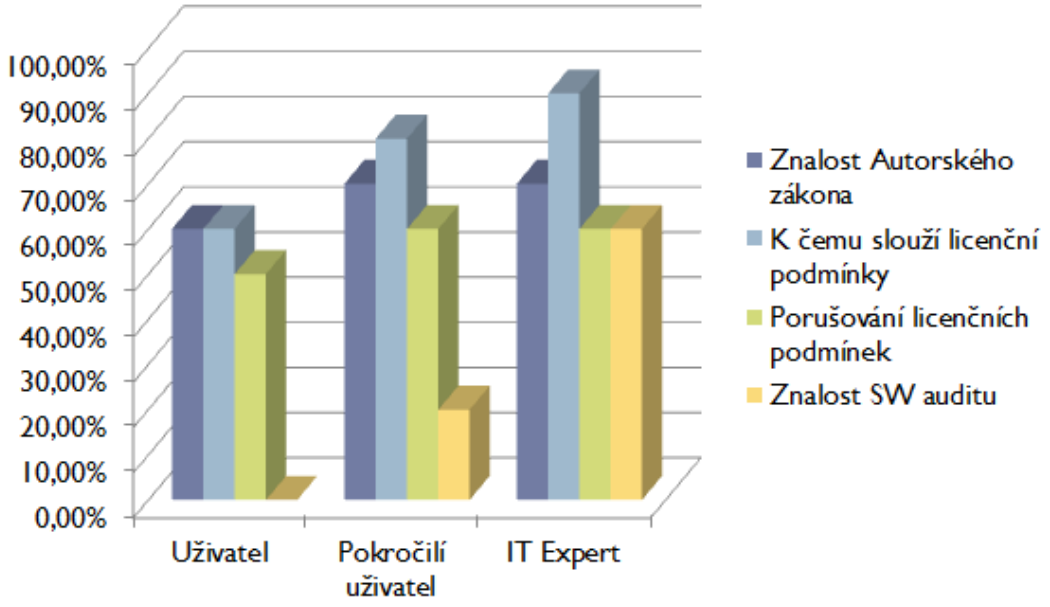
Provedl jsem průzkum mezi širší veřejností, IT administrátory a experty na informatiku. Cílem bylo získat data o chování lidí při porušování autorského práva. Zkoumal jsem, jak nakládají jednotlivci i administrátoři se softwarem a mediálními soubory chráněnými licenčním ujednáním. Dotazování jsem prováděl elektronickou i písemnou formou. Pro elektronickou formu jsem použil internetovou aplikaci od společnosti Google, jedná se o aplikaci Google Forms, která umožňuje elektronicky vytvořit dotazník, šířit ho po síti a následně generuje přehledný tabulkový editor s výsledky průzkumu.

Nejprve jsem rozdělil respondenty na uživatele, pokročilé uživatele, IT experty a administrátory. Kladené otázky se dotýkaly tématu autorského zákona. Zkoumal jsem znalost autorského zákona vztahující se k problematice licenčních podmínek, znalost vybraných základních typů licencí softwaru a funkčnost licenčních podmínek.

V druhé část jsem kladl otázky na respondenty, zda vlastní pouze legální software a mediální soubory, zda znají či používají jakýkoliv software na audit počítače pro přehlednost a zda považují za správné dodržovat licenční ujednání.

Celkem jsem oslovil bezmála sto respondentů, vyplněných dotazníků jak v papírové tak v elektronické podobě se mi vrátilo 68.

9.1 Výsledky dotazování



Obr2. Graf s daty

Z následujícího grafu se dá vyčíst velmi mnoho důležitých informací o znalosti a porušování autorského zákona. Znalost autorského zákona se pohybuje okolo 70% všech dotazovaných. Nutno podotknout, že valná většina odpověděla, že se s ním již setkala a zná jeho základy, ale nečetla jej.

V další časti - funkčnost licenčního ujednání - zde vidíme vzestup znalostí na základě odbornosti a orientaci v informatice.

Hrozivá fakta nám ukazuje znázornění zelených sloupců, týkajících se porušování licenčních podmínek. Stále patříme v tomto ohledu k nevyspělým zemím. Z celého výzkumu zhruba 60% respondentů porušuje licenční podmínky a tím i autorský zákon a vystavuje se riziku trestního stíhání. Nejčastěji k porušování autorského zákona dochází s ohledem na nelegální stahování softwaru a hudby z internetu a poté obcházení bezpečnostních prvků. V tomto ohledu vidím obrovský problém, kterým bychom se měli více zabývat.

Znalost a využití softwarových programů na provedení auditů je velmi nízká mezi běžnými uživateli. Tato fakta se dala předpokládat vzhledem ke znalostem licenčních podmínek, typů licencí a použití licenčního ujednání. V oblasti IT expertů jsem ale

očekával daleko větší procento znalostí, jelikož použití těchto programů značně usnadňuje kontrolu nad celou sítí počítačů a usnadňuje základní údržbu jednotlivých počítačů.

10 Závěr

Práce se skládá z teoretické a praktické části. V teoretické části jsem shrnul autorský zákon a důsledky trestního zákona z hlediska informační kriminality z oblasti porušování licenčního ujednání. Analyzoval jsem možné způsoby páchání trestné činnosti z oblasti šíření a přechovávání autorsky chráněných produktů (software), ale zároveň i možnosti ochrany a zabezpečení softwaru. Zkoumal jsem dosavadní postupy forenzní praxe při řešení autorského práva informační kriminality k danému tématu, spolupracoval jsem se specializovaným oddělením kriminální policie zabývajícím se danou problematikou. Provedl jsem analýzu používaných postupů při získávání dat o nelegálním softwaru a mediálních souborů z disku počítače.

V návaznosti na získané důležité informace jsem provedl průzkum u veřejnosti i u odborníků z oboru informatiky. Zkoumal jsem vztahy respondentů k licenčnímu ujednání, porušování autorského zákona a jeho znalost. Dále jsem vytvořil automatizační bezplatný postup pro získávání dat z bitové kopie disku pro forenzní analýzu za využití skriptu a operačního systému Linux verze Deft. Naprogramovaný skript je plně funkční a otestovaný. Dokládám ukázku výsledného reportu ve formátu spustitelném pro tabulkové editory.

V návaznosti na skript jsem vytvořil postup pro využití a sepsal celkovou dokumentaci i možnosti rozšíření, viz sekce možnosti rozšíření. Veškeré kladené cíle a požadavky na práci jsem splnil v plném rozsahu.

11 Reference

[1] The software alliance BSA. BSA. *The software alliance BSA* [online]. 2000, 2014 [cit. 2014-04-23]. Dostupné z:http://ww2.bsa.org/country.aspx?sc_lang=cs-CZ

[2] POLICIE ČR. *OKTE - historicky první policejní akreditované znalecké pracoviště v ČR* [online]. 2014 [cit. 2014-04-23]. Dostupné z: http://www.policie.cz/clanek/okte-historicky-prvni-policejni-akreditovane-znalecke-pracoviste-v-cr.aspx

[3] MANAGEMENT MANIA. *Forenzní analýza (Forensic Analysis)* [online]. 2011, 2013 [cit. 2014-04-23]. Dostupné z: https://managementmania.com/cs/forenzni-analyza-forensic-analysis

[4] FORMÁNEK. *Forenzní analýza počítače* [online]. Praha, 29.1.2007 [cit. 2014-04-23]. Dostupné z:http://service.felk.cvut.cz/anc/ofa/pub/doc/metodika.pdf. Seminární práce. ČVUT.

[5] AMIR JALILIFARD. *Peer to Peer File Sharing Through WCF* [online]. 2013, 2014 [cit. 2014-04-23]. Dostupné z:http://www.codeproject.com/Articles/614028/Peer-to-Peer-File-Sharing-Through-WCF

[6] JELÍNEK JELÍNEK & ETC. ALL. *Trestní zákoník a trestní řád s poznámkami a judikaturou*. Praha: Leges, 2013. ISBN 978-80-87576-69-4.

[7] LENKA HEČKOVÁ. *Česká protipirátská unie* [online]. 2008 [cit. 2014-04-23]. Dostupné z:http://www.cpufilm.cz/stories.html

[8] *Linux* [online]. 2004 [cit. 2014-04-23]. Dostupné z: http://linux.die.net/man/8/mount

[9] MICHAL BLAŽEK. *Programujte.com* [online]. 2006 [cit. 2014-04-23]. Dostupné z: http://programujte.com

[10] MINISTERSTVO KULTURY. *Přepisy zákonů* [online]. 2013 [cit. 2014-04-23]. Dostupné z: http://www.mkcr.cz/cz/autorske-pravo/zakon/predpisy-zakonu-7611/

[11] LIMBERK, Tomáš. Forenzní vědy a jejich využití v kriminalistice. Brno, 2011. Bakalářská práce. Právnická fakulta Masarykovy univerzity.

12 Přílohy

- exefinder.sh
- exefinder(1).sh
- out.csv
- out_media.csv