Využití forenzních metod pro odhalování počítačové kriminality a ochranu dat v kyberprostoru

Using forensic techniques to detect cyber crime and data protection in cyberspace

Bc. Martin Vašek

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Martin VAŠEK**
Osobní číslo:	**A11340**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Využití forenzních metod pro odhalování počítačové kriminality a ochranu dat v kyberprostoru**

Zásady pro vypracování:

1. **Vymezte základní pojmy a legislativu.**
2. **Popište vznik a historii počítačové kriminality.**
3. **Analyzujte formy a druhy počítačové kriminality.**
4. **Diskutujte o využitelnosti jednotlivých forenzních metod pro odhalování počitačové kriminality.**
5. **Vytvořte praktický příklad využití zvolené metody pro odhalování vybraných forem počítačové kriminality.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **JÍROVSKÝ, V. Kyberterorismus. ICTfórum/PERSONALIS 2006. [předneseno 27.9.2006]. Praha. (prezentace na konferenci -- nepublikováno).**
2. **RAK, R. Homo sapiens versus security. ICTfórum/PERSONALIS 2006. [předneseno 27.9.2006]. Praha (prezentace na konferenci -- nepublikováno).**
3. **Kyberterorismus roste závratným tempem. Novinky.cz [online]. 2006 [cit. 25.10.2006]. Dostupné na WWW: [http://www.novinky.cz/internet/kyberterorismus-roste-zavratnym-tempem_62464_hthrs.html].**
4. **Cyber-terorismus do dvou let realitou. Zive.cz [online]. 2006 [cit. 25.10.2006]. Dostupné na WWW: [http://www.zive.cz/h/Uzivatel/Ar.asp?ARI=119425].**
5. **BASTL, M. Jsou kolem nás či jen v naší mysli?: Kyberterorismus, Computer, leden 2003, roč. 10, č. 2, str. 67. ISSN 1210-8790.**
6. **BRZYBOHATÝ, M. - KROUPA, M. - HOS, M. - JANEČKOVÁ, B. - CHENÍČEK, J. - SLÁVIK, D. Terorismus a my, Praha: Computer Press, 2001. ISBN 80-7226-584-9.**
7. **BRZYBOHATÝ, M. Terorismus I. Praha: Police History, 1999. ISBN: 80-902670-1-7.**

Vedoucí diplomové práce: **Ing. Martin Hromada, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **8. února 2013**

Termín odevzdání diplomové práce: **3. června 2013**

Ve Zlíně dne 8. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Co je nejcennějším artiklem světa? Je to zlato? Jsou to peníze? Ne, jsou to informace!

Cílem této práce je nastínit nebezpečí a hrozby, které nám a našim datům hrozí v kyberprostoru, dále seznámit veřejnost o praktikách a metodách, které se běžně používají k ukradení, či jiné sabotáži našich dat počítačovými hackery.

Klíčová slova: forenzní metody, počítačová bezpečnost, kyberprostor, kriminalita, hacker, formy pirátství, vir, informační bezpečnost, informace, data.

ABSTRACT

What is the power that makes nowadays world around? Is it gold? Is it money? No, it is information!

The goal of this thesis is to sketch danger and threat of this kind of crime (i.e. with us and our data in cyberspace), then also to inform the public about technique and tricks that are used by black hackers to steal or sabotage our data.

Keywords: forenz method, computer security, cyberspace, criminality, blackhacker, types of piracy, virus, informational security, information, data.

Touto cestou bych rád poděkoval mému vedoucímu práce Ing. Martinovi Hromadovi Ph.D., za jeho ochotu, vstřícnost a odborné rady, které mi poskytoval během tvorby mé práce.

V neposlední řadě bych také rád poděkoval i mé rodině za dobré nervy a trpělivost v průběhu mého studia.

Zjistil jsem, že cokoliv se stane, jakkoliv zlé se to zdá - život jde dál a zítra to bude lepší.

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Téměř každý využívá informační systém prostřednictvím svého počítače (dále jen PC) a užívá ho ve své domácnosti. V dnešní době je to již neoddělitelná součást běžného života. Počítače ovlivňují náš každodenní život, a proto bychom si měli důležitá data chránit, jak před jejich ztrátou, tak před jejich zcizením nepovolanou osobou. Cílem této práce je částečně seznámit čtenáře se základními typy počítačových virů a způsoby různých útoků, které nám hrozí v kyberprostoru. Chtěl bych poukázat na možné riziko, které je s tím spojeno. Jak už zmíněnou ztrátou dat, zpomalením běhu počítače, znesnadněním práce na počítači, prozrazením citlivých informací, či zničením samotného hardwaru.

S vývojem technologií přichází na svět nový fenomén - kybernetická kriminalita, která je širokou veřejností ještě stále podceňována a ignorována. Za několik desítek let může být rozvíjející výpočetní technika stejně nebezpečná jako zbraně hromadného ničení.

Proto je třeba vyvinout důslednou a bezpečnou ochranu proti tomuto druhu trestné činnosti a vědět, jak se můžeme těmto útokům bránit se všemi právními postihy plynoucí z této nelegální činnosti.

I. TEORETICKÁ ČÁST

1 HISTORIE POČÍTAČOVÉ KRIMINALITY A BEZPEČNOSTNÍ HROZBY V KYBERPROSTORU

V dnešní době hraje bezpečnost důležitou roli. Stále více uživatelů se každý den setkává s hrozbami, které na ně působí. Co se skrývá v útrobách virtuálního světa? Jak těmto hrozbám úspěšně předcházet? Jaká rizika z těchto hrozeb pro nás plynou? Jakou škodu mohou představovat jak pro jedince, tak pro skupinu a společnost?

Každý z nás se již už určitě setkal s nějakým bezpečnostním problémem, zda už virem, "trojanem", spamem, nebo jiným podvodným útokem. Toto nebezpečí si nepřipouštíme a hrozby podceňujeme. Data jsou nejcennějším artiklem v digitálním světě. Kybernetická kriminalita má své opodstatnění v kyberprostoru. Kvůli vzrůstajícímu počtu této kyberkriminality vzniká interdisciplinární obor zabývající se nelegálními a škodlivými aktivitami kyberprostoru, jež jsou založeny na zneužití této technologie. Specializované pracoviště pro odhalování trestné činnosti je jedním z druhu ochrany, ale i jako prostředek k dopadení a usvědčení samotného pachatele. Personál je složen ze specializovaných vyšetřovatelů – **forenzních znalců.**

1.1 Historie počítačové kriminality

Historicky můžeme počítačovou kriminalitu klasifikovat do 3 základních časových etap. Jedná se o typická časová období, která mají své charakteristické rysy.

1.1.1 Počítačový pravěk

Tato časová etapa spadá do období, kdy ještě nebyly informační technologie příliš rozšířené, ale již zde můžeme sledovat první znaky počítačové kriminality.

Za první takový zločin je považován případ, který se udál v roce 1801 ve Francii. Tkadlec Jacquard sestrojil jednoduché zařízení, které dovolovalo automatizovat a pomocí děrných štítků opakovaně provádět jednotlivé úkony používané při tkaní speciálních látek. Jeho zaměstnanci „vynález" ze strachu před ztrátou zaměstnání nepřijali a následovala série sabotáží, které Jacquarda donutily od dalšího vývoje stroje upustit.

Dlouhý čas služby si krátili spojováním k sobě nepatřících hovorů a jejich jakoby

náhodným přerušováním. [8]

Počítačový věk je ale datován až 14. února 1946, kdy spatřil světlo světa první elektronkový počítač ENIAC. Tyto počítače měly ale úplně jiné specifikace a zabíraly i

celou místnost. Jejich cena byla astronomická a proto si je mohly dovolit jen velké korporace.

Jako první významný moment této etapy je upravování programů kvůli jejich nedokonalosti. Často bylo nutno zasáhnout přímo do zdrojového kódu programu a změnit tak výchozí naprogramování. Těmto zásahům se začalo říkat "hack" a programátorům, kteří začali zlepšovat programy hacker.

Další významný model počítačového pravěku je případ Cap `n` Crunch, Do dětských cereálií do se přidávala píšťalka, která vydávala zvuk o frekvenci 2 600 HZ, stejné jako používala telefonní společnost AT&T k vnitřní signalizaci v síti a ve spojení se zařízením Blue box. Této skutečnosti si všiml veterán z Vietnamu John Draper a přišel na to jak uskutečnovat hovory zdarma. Zveřejněním těchto závad se začala rozvíjet nelegální telefonie, která dostala název pheaking.

1.1.2 Počítačový středověk

Toto období je datováno r. 1981 uvedením prvního počítače typu IBM PC na trh. Dle jeho velikosti a napájecích možností se dalo usoudit, že se masově rozšíří mezi běžné uživatele.

Se změnou techniky se mění i typičtí pachatelé Prvními pachateli jsou počítačoví fandové, kteří berou průnik do systému jako výzvu a snaží si dokázat, že žádný systém není "neprůchodný".

Pro počítačový středověk je charakteristický nástup počítačových virů, nejčastěji trojských koňů, kteří se chovali jako fungující program, ale ve skutečnosti to byla jen "zástěrka". Tento infiltrační nástroj prováděl svou škodlivou činnost v pozadí.

Další charakteristický rys tohoto období spočívá v rozvoji technologií, konkrétně CD-R mechanik, což umožnilo to, aby se každý uživatel mohl stát počítačovým pirátem.

1.1.3 Počítačový novověk

Přestože ve středověku počítačová kriminalita zažívá prudký vzestup, v novověku jsou tyto metody "dotaženy" k dokonalosti a to kvůli rozvoji informačních technologií a masivnímu rozšíření internetu a klientských PC. Počítačové viry se již objevují stabilně a jejich nebezpečnost je čím dál vyšší.

Významnou změnou byla změna k přístupu dat, když byl dříve internet organizován na přístupu klient/server a cílová data musela být umístěna na některém cílovém serveru,

(dala se tedy snadno vymazat). Nyní můžeme využít připojení tzv. peer-to-peer. U tohoto připojení nepotřebujeme pro přenos dat cílový server, ale jsme připojeni k cílovému uživateli, který nabízí daný obsah.

1.2 Kyberprostor

Kyberprostor je jako pomyslná spojnice mezi virtuálním světem a realitou. Všechny aktivity se uskutečňují prostřednictvím počítačových a telekomunikačních sítí a počítačových systémů. Realita je zprostředkována uživatelem, který určuje příkazy. Mezilidské aktivity se pomalu vyměňují za informační systémy a sociální sítě. Ve 21. století je vytvořen globálně z infrastruktury sítí, které jsou mezi sebou propojené a navzájem na sebe závislé. I nejmenší výpadek jakékoli infrastruktury může způsobit škody velkého rozsahu. Když selže např. letecká infrastruktura nebezpečí je extrémní, jde o životy, neboť řídící centra podléhají kyberprostoru.

Každý z nás si může prostřednictvím PC individuálně vyměňovat názory, sdílet informace, poskytovat sociální podporu, vytvářet videa, webové stránky, hrát počítačové hry přes internet, nakupovat a zapojovat se do politických diskusí s použitím globální sítě. K tomu všemu je zapotřebí počítačová síť, a to s sebou nese riziko útoků na naší pracovní stanici a naše data.

Obrázek 1 kyberprostor [22]

1.2.1 Kyberkriminalita

Kyberkriminalitou myslíme takovou činnost, která je v rozporu se zákonem a je páchána v kyberprostoru pomocí počítače. Zahrnuje jevy jako počítačovou kriminalitu, informační

kriminalitu, softwarové pirátství, kybernetický terorismus, politickou a hospodářskou špionáž, extrémní politickou nebo teroristickou propagandu, či jiné nebezpečné aktivity jako jsou krádeže hesel, porušení autorského práva, finanční podvody, útoky na servisní sítě, krádež duševního vlastnictví až upozorňování na sebe sama, sabotáže, získání citlivých dat a jinou trestnou činnost.

Časem se postupně zlepšovaly i techniky hackerů, a to i "díky" rozvoji technologií, které jim umožnily využívat větší škálu možností. V minulosti vznikal spíše škodlivý software, který měl za úkol pouze sabotáž, avšak v průběhu let se změnily i trendy a lidé v tomto oboru začali vidět vidinu zisku a možnost se obohatit.

Jak v reálném světě, tak i v kyberprostoru zanechává pachatel stopy, podle kterých se dá vypátrat. Vyšetřování však musí proběhnout co nejdříve, čím dříve začne, tím je větší šance na vypátrání pachatele, ale ani to nemusí být vždy průkazné. Hackeři používají mnoho metod šifrování a skrývání svých útoků za nic netušící uživatele, od nichž útoky probíhají a útočník vše vzdáleně řídí klidně i z druhého konce světa.

Dalším závažným problémem je také nedokonalost našeho právního systému, který nedokáže efektivně stíhat pachatele. Jen "malá hrstka" ilegálních činností je odhalena a viník je stíhán, neboť prokazování viny je velmi obtížné a pracné.

Útočník pracuje v globálním prostředí, může být kdekoliv na světě, kde má přístup k síti. Je zpravidla vždy o krok napřed, protože může použít různé algoritmy či šifry, aby skryl nebo přesměroval místo svého útoku. Může „maskovat" i za skupinu počítačů a tak je extrémně obtížné ho vystopovat. Útočníci bývají navíc zpravidla nadprůměrně inteligentní.

Obrázek 2 kyberkriminalita [23]

1.2.2 Kyberválka

S rozvojem technologií se rozvíjí i praktiky a zájmy útočících stran. Válka se už nevede jen v reálném světě, ale začíná se přesouvat do virtuálního prostředí, protože mnoho řídících systémů podléhá právě počítačům. S nadsázkou můžeme říci, že počítačové systémy spravují téměř všechna klíčová odvětví.

Časopis „The Economist“ popisuje kybervojnu, jak novou generaci války**.** Novodobý pojem je odvozen od kyberkriminality. Jsou do ní zapojeni jednotlivci, organizace a státy.

Kyberválku můžeme rozdělit dle několika hrozeb: špionáž, sabotáž, vyřazení soupeře. Hlavním cílem je dnes hlavně armáda, technologie, know how korporace, civilní prostředí.

Příkladem je společnost WikiLeaks, jenž zveřejňovala tajné skutečnosti. Vlády začaly jednat a “odsřihly“ ji od webu a “zmrazily“ konta, aby společnost ukončila svou činnost.

Hackeři z celého světa se později spojili a začali útočit silou společného útoku na organizace, které mohly za odstavení od webu např. Visa, Paypal ...

V takovémto konfliktu není velikost, jak je tomu zvykem vždycky výhodou, v kyberválce je to spíše naopak. Útoky nemusí být příliš nákladné, internet byl vyvinut především kvůli užívání než na bezpečnost a to dává výhodu útočníkům. Ani velikost není rozhodující, spíše naopak, větší státy bývají spíše zranitelnější i menší státy mohou hrát klíčovou roli.

Časem by to mohl sice změnit tzv. “reinženýring“ (podstatně předělaný systém) některých klíčových systémů pro větší bezpečnost, ale zatím tomuto scénáři nic nenasvědčuje, větší strana má handicap při odzbrojování, či okupaci území.

Obrázek 3 kyberválka [22]

1.2.3 Kyberterorismus

S narůstajícím počtem útoků přes PC by všechny země světa měly brát tuto hrozbu vážně a posílit bezpečnost klíčových systémů.

V dnešní době, kdy je tato disciplína poměrně nová, nejsou bezpečnostní opatření dostatečná, a proto vzniká "prostor" pro tento nastupující sofistikovaný druh terorismu využívající složité operace.

Kyberterorismus je ilegální formou teroristického útoku, která je realizována pomocí počítačové sítě. Je to promyšlený politicky motivovaný útok proti informacím počítačových systémů, (např., útok "virusu Stuxnet," jenž zamořil celý íránský jaderný program).

Virtuální síť může být ale pouze sekundárním cílem, protože primárním cílem je systém napojen na fyzické zařízení, což může vést až ke zničení daného zařízení a posléze ke ztrátám na lidských životech.

Skupiny využívají různé sofistikované metody komunikace, aby se dohodly, kdy má dojít

k útoku. Profesionálnější programy slouží k zakódování map a souřadnic. Typickou obětí kyberterorizmu se stal Izrael, Írán, Severní Korea, USA, Rusko, atd.

Obrázek 4 kyberterorismus [22]

1.2.4 Kyberšikana

Termínem kyberšikana označujeme všechny nebezpečné komunikační jevy, které jsou realizovány prostřednictvím informačních, nebo komunikačních technologií. Je to druh psychické šikany, který má za následek ublížení, anebo jiné poškození oběti, ať již cíleně a promyšleně, nebo z nevhodného vtipu a nedomyšlení následků, které mohou později nastat.

Ve virtuálním prostředí může k útoku dojít kdykoliv a kdekoliv a útočník bývá většinou anonymní, skrytý za tzv. "nick", což je jeho přezdívka ve virtuálním světě. Tato skutečnost smazává rozdíly mezi věkem a pohlavím.

Může jím být téměř každý, kdo má základní znalosti o informačních a komunikačních technologiích.

V tomto druhu šikany nedochází k osobnímu kontaktu a oběť a útočník se nemusí ani osobně znát a kvůli nedostatku zpětné vazby se útočníci stávají agresivnější a nelítostnější.

Zatímco v běžném životě pomluvy a posměšky časem "vyhasnou", v kyberprostoru se daný zesměšňující materiál šíří daleko rychleji, a tak si ho může každý prohlédnout.

Dopad na jedince může být stejně skličující jako u klasické šikany, s tím rozdílem, že zde oběti po těle nemají modřiny a šrámy, ale jejich újma je psychická a může vést až k nejhoršímu.

Prvním zveřejněným případem kyberšikany je teprve čtrnáctiletý student Ghyslain Raza z Kanady, který natočil sám sebe při předvádění bojové scény z hvězdných válek. Tuto nahrávku mu později spolužáci odcizili a umístili na youtube. Tato nahrávka obletěla mnohokrát celý virtuální svět a začalo vznikat mnoho webů, kde byl chlapec zesměšňován. Ghyslain se z toho psychicky zhroutil a musel se podrobit dlouhodobé léčbě.

Obrázek 5 kyberšikana [21]

Nejčastějším projevem kyberšikany je publikování kompromitujících, či ponižujících materiálů, pomlouvání, kradení identit a následné rozesílání různých e-mailů smyšleného často vulgárního nebo sexuálního charakteru např. kontaktům oběti, ztrapňování pomocí falešných profilů, napadání a urážení na veřejných chatech, zveřejňování osobních informací s cílem poškodit, vyloučení z virtuálních komunit a obtěžování pomocí počítačových systémů.

Jak předcházet kyberšikaně:

a) chovat se s úctou ke všem, respektovat je

b) nebýt příliš důvěřivý

c) nikdy nesdělovat osobní a citlivé informace

Obrana proti kyberšikaně:

a) neoplácet útoky

b) blokovat služby – zamezit útočníkovi přístup, vše včas oznámit administrátorům daného webu

c) odhalit pachatele – mnoho pachatelů odradí právě prozrazení jejich identity

d) oznámit vše dospělým

e) být všímavý k okolí – když v okolí probíhá šikana

f) podpořit oběti – poradit jim kam se mají obrátit, popřípadě co mají dělat

1.3 Účastníci kyberprostoru

V kyberprostoru bychom měli rozlišovat účastníky, kteří se v něm vyskytují. Identifikovat je můžeme pomocí IP adresy, ať již veřejné či neveřejné, či uživatelského jména. Všichni uživatelé, kteří se pohybují v kyberprostoru, komunikují s ostatními uživateli a běžně se mohou jejich cesty "zkřížit pomocí" počítačové sítě.

Osoby, které se vyskytují, ve virtuálním světě dělíme na:

a) Basic users (uživatelé)

b) Hackeři

c) Crackeři

d) Bezpečnostní specialisté

a) Terčem útoků se nejvíce stávají právě **obyčejní uživatelé**, protože jsou pro tyto útoky nejsnadnějším cílem a kvůli své nevědomosti téměř nikdy neodhalí, že byli napadeni počítačovým útočníkem. Takovýto uživatel má jen základní znalosti o informačních technologiích a je schopen pracovat pouze v základním uživatelském rozhraní, tzn. např. ve windows pomocí myši a nikoliv v textovém rozhraní pomocí příkazů, které vyžadují již rozšířené znalosti ICT. Představuje největší nebezpečí sám sobě, neboť nezná metody počítačových hackerů a namísto toho, aby se snažil zabránit útokům, tak ještě spolupracuje a sděluje své citlivé informace, a "kliká" na nebezpečné odkazy, které na nás "číhají" po celém webu.

b) Hackeři mají již vysokou znalost informačních technologií a patří k pokročilým uživatelům. Většinou to bývají vysoce inteligentní lidé, kteří se řídí vlastními pravidly a zásadami a nerespektují zákony a často patří k nějaké komunitě. Tito bývají obvykle uzavření reálnému okolí a svůj život žijí spíš na "půdě" virtuální.

Tento pojem se původně váže zhruba k 50. letům 20. století. Nazývají se radioamatéři a hledají nové metody ke zlepšení svého vysílače. Počátky slova hacking jsou z angloamerického výrazu a myslí se tím nenucená procházka na americké universitě MIT (Massachusetts institute of technology), kde se takto označovalo řešení problému, a to hravě a rychle.

Hackera definuje jeho schopnost do detailu pochopit všechny programovatelné systémy a snažit se je vylepšit, či obejít. Tento uživatel si programuje a vytváří si vlastní skripty a dokáže naplánovat složité postupy, které mu zesnadní jeho pohyb v kyberprostoru. Bývá samouk-amatér a všechny své znalosti získává pomocí internetu a je zdatný v bezpečnostních opatřeních.

Hackery můžeme dělit do 3 hlavních skupin, "**Dobří hackeři**" se snaží opravovat chyby a nepřesnosti na webu a po jejich zjištění kontaktují administrátora a spolupracují s ním na jejich odstranění.

Agresivní hackeři patří k aktivním hrozbám virtuálního prostředí, často jsou označováni jako **"Black hackers"**. Pracují stejně jako "dobří "hackeři s tím rozdílem, že se systém snaží nabourat, či nějak jinak sabotovat. Výhody, které tímto vzniknou, se snaží využívat pro sebe, anebo je někomu později prodat za peníze.

Neutrální hackeři jsou někde na rozmezí mezi "dobrými a zlými" hackery. Většinou neví kam se zařadit, jde o morální zásady, kam až daleko jsou schopni zajít.

Je mnoho známých hackerů, kteří spáchali činy, které byly vyčíslené v řádech stamilionů dolarů. Nejznámějším z nich je asi **Kevin David Mitnick**, kterému byla vyčíslena škoda, kterou způsobil v řádu 300 milionů dolarů. V současnosti vlastní svou bezpečnostní firmu Mitnick Security Consulting.

c) Crackeři se zaměřují především na prolomení ochrany, jak už cizích sítí, wi-fi sítí, nebo bezpečnostních opatření softwaru. Na rozdíl od hackerů, jsou pro běžného uživatele přínosem, protože se o své know-how většinou dělí a dávají k dispozici sériové klíče, či generátory klíčů, takže uživatel nemusí registrovat drahé počítačové

hry a programy. Jejich činnost však způsobuje obrovské finanční ztráty vývojářským filmovým týmům a vydavatelským společnostem ve video-herním průmyslu.

Kyberpolicie nemá dostatek prostředků k zamezení této činnosti, hlavně z důvodu, že bývají většinou velmi zkušeními uživateli, často i lidé přímo z praxe, a to především v otázkách bezpečnosti informačních systémů, proto je těžké je vystopovat.

d)Phreakeři jsou hackeři, zaměřující se na GSM sítě, hlavně na telefony a telefonní ústředny. Volají zdarma pomocí chyb a nepřesností, které se v GSM sítích vyskytují. Zaměřují se především k odposlechu sítí a využívání GSM sítí k volání, ale mohou klidně "nabourat" i náš telefon. Obzvlášť dobrý pozor je třeba si dávat na neznámá čísla. Když se na ně snažíme zavolat zpět, jsme přesměrování na službu za vysokou cenu.

Proti těmto útokům je nepoučený uživatel takřka bezbranný, protože hovor prokazatelně uskutečnil a mimosoudní náhrada je téměř neskutečná, proto bych rád zdůraznil, aby si uživatelé dávali dobrý pozor a **volali jen na známá telefonní čísla.**

Obrázek 6 hacker

2 TYPICKÉ FORMY PÁCHÁNÍ POČÍTAČOVÉ KRIMINALITY

Počítačová kriminalita zahrnuje neoprávněné nakládání s počítačovými programy, jejich programovým vybavením, či jejich užívání v rozporu s licencí, dokumenty a ostatními daty, které jsou právně chráněné.

Tato činnost nemusí být ale jen v odcizování dat, či ilegálních kopie nějakých programů, už jen samotný neoprávněný vnik do cizí sítě se považuje za trestný čin.

Tyto formy mají vždy jedno společné a to je zneužití výpočetní techniky, která má vzhledem ke svým specifickým vlastnostem dominantní postavení ve všech klíčových systémech.

Počítačová kriminalita, dle mezinárodní Budapešťské úmluvy o počítačové kriminalitě z 23. 11. 2001, (Convention on Crime, kterou Česká republika podepsala 9. 2.2005), by se dala tedy rozdělit na jednotlivé oblasti.

1. Trestné činy proti důvěřivosti, integritě a dostupnosti počítačových dat a systémů

- neoprávněný přístup
- neoprávněný odposlech
- narušování dat
- narušování systémů
- zneužívání zařízení

2. Trestné činy se vztahem k počítači

- počítačové padělání
- počítačový podvod

3. Trestné činy se vztahem k obsahu počítače

- dětská pornografie
- rasová či etnická diskriminace
- násilí proti skupině, či jedinci

4. Trestné činy související s porušováním autorského práva a souvisejících práv

Další rozdělení je možné stanovit, dle mínění známého odborníka, pedagoga a soudního znalce v oboru výpočetní techniky pana Prof. Vladimíra Smejkala, jenž rozděluje počítačovou kriminalitu do dvou základních skupin, a to na:

- Delikty, kde počítač, program, data, informační systém apod. jsou nástrojem trestné činnosti pachatele,
- delikty, kde počítač, program, data, informační systém atd. jsou cílem zločinného útoku, přičemž se může jednat o tyto trestné činy:
    - fyzický nebo logický útok na počítač nebo komunikační zařízení,
    - neoprávněné užívání počítače nebo komunikačního zařízení,
    - neoprávněné užívání nebo distribuci počítačových programů,
    - změnu v programech a datech, okrajově i v technickém zapojení počítače nebo komunikačního zařízení,
    - neoprávněný přístup k datům, získávání utajovaných informací (tzv. počítačová špionáž) nebo jiných informací o osobách (osobní údaje),
    - trestné činy, předmětem jejichž útoku je počítač jako věc movitá. [5]

2.1 Důležité zákony v oblasti počítačové kriminality

Nový trestní zákoník č. 40/2009 Sb. zavádí v problematice počítačové kriminality změny stávajících skutkových podstat trestných činů, případně některé skutkové podstaty zcela nové, dosud nevypracované.

Na rozdíl od stávající právní úpravy vychází nový TZ, pokud jde o úpravu počítačové kriminality z Úmluvy o počítačové kriminalitě ze dne 8. 11. 2001, kterou Česká republika podepsala v roce 2005.

2.1.1 § 182 Porušení tajemství dopravovaných zpráv

(1) Kdo úmyslně poruší tajemství

a) uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením,

b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo

c) neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data,bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

(2) Stejně bude potrestán, kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch

a) prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu, telefonního hovoru nebo přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu, nebo

b) takového tajemství využije. [9]

Nová právní úprava tohoto trestného činu je rozsáhlejší, neboť vedle uzavřeného listu nebo jiné písemnosti dopravované poštovní nebo jinou dopravní službou zavádí datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací, jenž jsou přiřaditelné k identifikovanému účastníkovi nebo uživateli, který zprávu přijímá a neveřejný přenos počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektronického vyzařování z počítačového systému, přenášejícího taková data.

2.1.2 § 230 Neoprávněný přístup k počítačovému systému a nosiči informací

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,

c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo

d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,

bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty. [9]

Podíváme-li se na strukturu § 230, pak je především zřejmé, že celé ustanovení směřuje k ochraně informací uložených v počítačovém systému.

Toto ustanovení upravuje postih překonání bezpečnostního opatření a současně neoprávněného získání přístupu k počítačovému systému a případně další jednání pachatele (např. hackera), který již získal přístup k počítačovému systému nebo k nosiči informací.

2.1.3 § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo

b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části, bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo jiné majetkové hodnoty nebo zákazem činnosti. [9]

K naplnění skutkové podstaty tohoto trestného činu není zapotřebí toho, co v předchozím případě, tedy získat přístup k informačnímu systému a provádět manipulaci s uloženými daty, zde pouze postačí, pokud si pachatel zajistí nebo přechovává zařízení softwarového vybavení, heslo, přístupový kód, apod., to vše v úmyslu spáchat tento trestný čin.

2.1.4 § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

(1) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté

a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo

b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat, a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty. [9]

Účelem tohoto ustanovení je postihnout hrubou nedbalost správců sítě, apod., neboť škoda, kterou tito pracovníci mohou způsobit pochybnou prací, je daleko větší, než např. útok hackera. Postihováno tak nebude pouhé neúmyslné jednání nebo omyl, nýbrž i hrubá nedbalost.

2.1.5 § 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.

(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. [9]

Otázka postihů za porušení autorského zákonu upravuje § 270 trestního zákoníku řešící porušení autorského práva, práv souvisejících s právem autorským a práv k databázi. V odstavci 1 tohoto ustanovení se uvádí „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 2 léta zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

Trestné činy proti duševnímu vlastnictví se velmi rozšířily zejména rozmachem internetu. Mezi faktory, které k tomu přispěly, lze zařadit zejména:

1) kopie může být pořízena během krátké doby a s poměrně nízkými náklady
2) specifika autorských práv spočívající v jejich nehmotné podstatě
3) vysoká cena SW vybavení

Mezi nejčastější porušování autorského zákona lze zařadit zejména kopírování díla. Zdánlivě a vzhledem k nehmotné podstatě duševního vlastnictví nevzniká žádná přímá škoda, protože vlastník neutrpí žádnou újmu, jeho dílo není nijak poškozeno. Nicméně z hlediska autorského zákona (zák. č. 121/2000 Sb., v platném znění) je i kopírování díla jednak samo o sobě jeho užití a jednak obvykle vede k dalšímu neoprávněnému užívání díla.

Typickým porušením autorského zákona je neoprávněné šíření díla, zejména nyní, po internetu. Jde zejména o tyto postupy:

- vystavení díla na webové stránky
- použití FTP a podobné služby určené k přenosu souborů
- prostřednictvím elektronické pošty
- v sítích peer to peer, které jsou silným prostředkem pro ilegální sdílení a výměnu dat

Mezi poměrně časté porušení autorského zákona patří zásah do díla nebo jeho úprava. Jasným porušením autorského práva bude tak například odstranění bezpečnostních prvků chránících program před zneužitím nebo odstranění identifikačních prvků programového díla.

Dalším typickým porušením autorského zákona je neoprávněné užití díla. Pokud jde o programové produkty díla, bývá dosti velkým problémem prokázání neoprávněného užití díla, pokud k němu nedojde přímým zneužitím celé nelicencované aplikace. Programy publikované jenom v uzavřené spustitelné verzi je obvykle obtížné využít, avšak u programů s dostupným kódem nemá pachatel žádné problémy s jeho získáním.

2.2 Trestné činy proti důvěrnosti a integritě a dosažitelnosti počítačových dat

Takovýto útok nesměřuje na cílový předmět, tedy počítač, ale na jeho programové vybavení a data. Tuto nezákonnou činnost dříve postihoval § 257a tehdejšího trestního zákona (zákona č. 140/1961 Sb.), který byl nahrazen novým trestním zákoníkem (zákonem č. 40/2009 Sb.), jenž ve svých ustanoveních §§ 230 – 232 postihuje již samotnou manipulaci a neoprávněný vstup do počítače, či počítačové sítě uvedeno výše.

2.2.1 Neoprávněný přístup k počítačovému systému a nosiči informací

Útočník se snaží nezákonně připojit na předem určený počítač, či počítačovou síť a celou její databázi. V první řadě musí útočník prolomit nějaké bezpečnostní opatření. Většinou se jedná o heslo do systému a adresu počítače, kterou se pokusí vzdáleně nebo lokálně napadnout.

K získání těchto informací se používá různých metod, ať je to **sniffing** (“tichý odposlech“), nebo podstrčením nějakého škodlivého softwaru (dále jen SW), který heslo zjistí a umožní tak vzdálený přístup k počítači, či nepozorovaně pošle na předem domluvenou adresu (nejčastěji se na to používají zvláštní typy “trojských koní“, tzv. password-trojani, kteří mají za úkol jediné, zjistit heslo a předat ho útočníkovi předem nastaveným způsobem.

S nezákonným přístupem je také velmi často spojován tzv. **hacking**, což je neoprávněný průnik do konkrétního informačního systému, provedený zvnějšku, zpravidla ze vzdáleného počítače. Samotný průnik je samozřejmě podmínkou pro další neautorizovanou činnost v rámci cílového systému. Pachatelé se většinou nepřipojují k objektu útoku (počítači) přímo, ale přes jeden i více internetových serverů v různých částech světa. Cílem takového postupu je podstatné snížení možnosti identifikace skutečného umístění počítače, který byl při útoku užit. [6]

2.2.1.1 Sociální inženýrství

Další a asi nejjednodušší metodu využívá sociální inženýrství, které spoléhá na omylnost lidského faktoru. Tato metoda nepotřebuje žádné složité zařízení ani speciální um v oblasti informačních technologií. Jde o to zeptat se, využít umění lstivosti a nedůslednosti lidí, tedy zaměstnanců, kteří klíč ke vstupu do systému znají. Nejčastěji se tato metoda provádí pomocí telefonu nebo jiných komunikačních zařízení, většinou z pohledu síly (šéf, administrátor, policie ..), který neprodleně potřebuje znát přístup do systému a po telefonu

vyhrožuje, že když okamžitě informace nedostane, tak můžeme přijít např. o zaměstnání aj. Nezkušená osoba "pod tlakem" často tyto interní informace raději sdělí a bezpečnost našeho systému může být vážně narušena. Proto bychom měli své zaměstnance včas proškolovat a seznámit je se situacemi, které mohou nastat.

2.2.2 Neoprávněný odposlech – sniffing

Sniffing je technika, při které dochází k ukládání a následnému čtení TCP paketů. Používá se zejména při diagnostice sítě, zjištění používaných služeb a protokolů a odposlechu datové komunikace.

Rozhněvaný zaměstnanec firmy nebo hacker může umístit odposlouchávací jednotku na strategické místo a odposlouchávat firemní komunikaci, např. mezi vývojovým oddělením a vedením firmy. Tyto informace může poté zpeněžit u konkurenční společnosti. Obdobně může vedení firmy odposlouchávat své zaměstnance a kontrolovat jejich činnost.

Pro odposlech datové komunikace (sniffing) existuje hned několik způsobů, ale de facto ke každému typu odposlechu je zapotřebí sniffer, softwarové vybavení (a v jistých případech i upravený hardware), které takové odposlouchávaní umožní. [6]

2.2.2.1 Sniffing v drátových síťích

Tento druh odposlechu je podstatně jednodušší než u bezdrátové sítě Wi-Fi. Provádí se pomocí speciálního SW pro správu sítě. Velkým bezpečnostním rizikem se může stát např. rozhněvaný administrátor, či správce sítě, který může cílový systém ohrozit velmi snadno. Tito zaměstnanci měli být velmi loajální a profesionální. Z tohoto důvodu je důležité dávat velký pozor na to, koho přijímáme do zaměstnání. Když do naší firmy nastoupí někdo s úmyslem sabotovat a sledovat provoz a komunikaci celé společnosti, bude těžké takového sniffera odhalit. Takovýto zaměstnanec má většinou i přístupová práva ke správě celého systému a potřebnou počítačovou dovednost, aby celou svou záškodnickou činnost "uklidil". T tohoto důvodu firmy většinou najímají dva správce sítě, aby byla možná kontrola i těchto zaměstnanců.

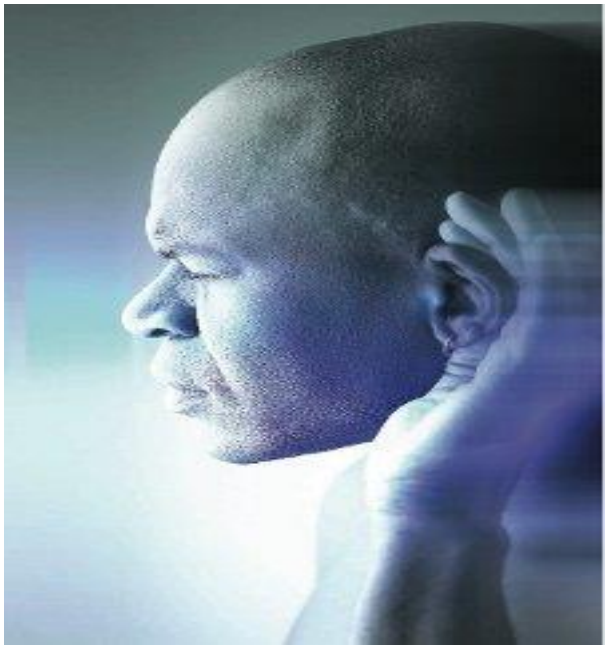
2.2.2.2 Fyzický odposlech – Man in the Middle

Dalším snadný způsob, jak se dostat k interním informacím, je fyzický (hardwarový) odposlech Man in The Middle. Tento způsob mohou využít všichni pracovníci, kteří mají fyzický přístup k topologii sítě, může to být tedy klidně údržbář, či uklízečka. K takovéto sabotáži postačí jen notebook se dvěma sítovými kartami, nebo odposlouchávací můstek a

přímý přístup k uzlům a síti. Proto by měly být všechny tyto fyzické přístupové body do sítě řádně zabezpečeny.

2.2.2.3 Lokální sniffing

Další metodou je odposlech sítě přímo, tedy lokálně. Sniffer se nemusí vyskytovat mezi dvěma počítači, ale stačí, aby se nacházel mezi TCP/IP ovladačem systému a síťovým hardwarem (kartou), na PC vybrané oběti. Útočník k tomuto sběru informací využívá opět vybraný SW (většinou low-level), který sbírá data a ukládá je, nebo rovnou přeposílá útočníkovi. Jelikož je tento škodlivý SW nainstalován na cílovém počítači, musel by být na zařízení nainstalován přímo, nebo vzdáleně. Obranou proti vzdáleným útokům je mít dobře nakonfigurovaný firewall a antivirový SW a mít nastavené bezpečné heslo (min. 15 místné). **Nevzdalovat se od PC, když je zapnutý!**



Obrázek 7 sniffing [6]

2.2.3 Narušení dat

Útoky, které směřují k zneužití dat a ostatních informací za účelem zisku, či jiných důvodů, se řadí k formě počítačové kriminality a jsou trestné. Tato forma kriminality může mít dalekosáhlé následky. Tyto útoky řadíme dle následujících kritérií:

- zneužití osobních (personálních) informací, může způsobit vážné újmy jak morální, tak i hmotné,

- zneužití obchodních informací průmyslového charakteru může mít vážný vliv na celkovou prosperitu a celkový vývoj dané organizace. Tyto informace mohou být pro podnik klíčové (know-how) a mít dopad na celý chod podniku, jak na firmu celkově, tak na zaměstnance, kterým tak hrozí ztráta zaměstnání,
- obchodní machinace – manipulace s daty finančního charakteru, např. obohacování se z jiných účtů, které jsou prováděny virtuálně. Postižená osoba může být jednotlivec, či celá organice, peněžní ústav aj.

2.2.4 Narušení systému

Tato forma kriminality je úzce spjata s nezákonným přístupem. Nezákonný přístup znamená snahu útočníka proniknout do systému. Útočník vniká do systému hlavně z těchto důvodů:

- pouze vnikne do systému, kvůli svému egu, aby dokázal jak je schopný a překonal všechny bezpečnostní nástrahy tvůrce systému, s daty v systému ale nepracuje,
- nakládá s těmito získanými daty ke svému prospěchu, data si může zkopírovat a dále s nimi např. obchoduje. Tento útok je ale **nedestruktivní.**
- data změní nebo zničí, popřípadě nahradí fiktivními. Tento útok je tedy **destruktivní**.

2.2.5 Zneužití zařízení

Zneužití zařízení spočívá v tom, když je cílový počítač, či programové vybavení využíváno bez souhlasu majitele k jiným účelům, než bylo původně určeno. Hacker se tedy může vzdáleně připojit na počítač, za který se "maskuje" a přes tento počítač páchá trestnou činnost. Tato činnost se jen velmi často odhaluje, protože útočník má plnou kontrolu nad PC, ale pracuje tzv. v pozadí, takže si toho majitelé PC často vůbec nevšimnou.

2.3 Trestné činy spojené se vztahem k PC

U těchto trestných činů se považuje za prostředek k páchání trestné činnosti počítač. Útočník se nezaměřuje na obsah (data) počítače, ale používá počítač, či jinou informační technologii pouze k dosažení svých záměrů.

2.3.1 Počítačové padělání

Zde se jedná převážně o hospodářskou trestnou činnost. Tyto trestné činy se týkají nejčastěji padělání měny a trestných činů daňových. Jedna z nejčastějších forem z trestných činů spojených s PC jako prostředku k páchání trestné činnosti je dle zák. §§ 233 – 239 TZ padělání a pozměňování peněz, platebních karet, kolků, aj. ochranných známek k dokazování pravosti. Takováto trestná činnost může být spojena i s jinou počítačovou kriminalitou např. s phishingem, kde jsou od nic netušících uživatelů zcizeny přihlašovací údaje včetně kódů ke kontu a pomocí zfalšovaných karet může pachatel vybírat obnos přímo z bankomatu.

2.3.2 Počítačový podvod

Mezi počítačové podvody můžeme zařadit velké množství trestných činů, které jsou nad rámec této práce, ale určujícím rysem počítačového podvodu je zneužití PC, nebo jiné výpočetní techniky jako prostředek trestné činnosti. Všechny tyto činnosti, ale mají podobný znak, a to snahu oloupit danou osobu o zisk (téměř vždy peníze).

2.4 Trestné činy se vztahem k obsahu počítače

Tato kategorie trestné činnosti by se dala kategorizovat do 2 hlavních skupin a to je uchovávání zakázaných dat a zpřístupňování a šíření těchto dat.

Předmětem těchto dat bývá většinou pornografie, především dětská, kterou řeší zák. §191 a násl. TZ a soubory obsahující podněcování, nabádání, či propagace nenávisti k různým etnickým, rasovým, či náboženským skupinám a případy extrémistických skupin propagující své nezákonné aktivity, spolu s případy xenofobie.

2.5 Trestné činy se vztahem k autorským právům

Tato trestná činnost také jinak nazývána **počítačové pirátství**, je trestná činnost, která se vztahuje k porušování autorských práv. Rozumíme tím všechny útoky na právo autora a další práva k počítačovým programům, které jsou uvedeny v autorském zákoně

Dle § 270 trestního zákoníku můžeme autorský zákon porušit těmito způsoby:

a) Užívání programového vybavení bez licence, popřípadě na více pracovních stanicích než bylo dohodnuto.
b) Zasahováním do programu a provádění neoprávněných změn

c) Šíření, či poskytování SW jiným osobám, než je uvedeno v licenčních podmínkách.

2.5.1 Neoprávněné užívání SW

Tuto trestnou činnost dělíme hlavně podle toho, zda-li uživatel používá SW, či media pro svou vlastní potřebu, či komerčně za účelem zisku.

2.5.1.1 Neoprávněné užívání SW uživatelem pro vlastní potřebu

V ČR je tato forma kriminality ze všech nejrozšířenější. Tvorba ilegálních kopií SW, či filmů je u nás běžným zvykem a skoro nikomu nedochází, že se dopouští trestného činu proti autorským právům.

2.5.1.2 Užívání nelegálního SW pro komerční účely

V komerční sféře také dochází k zneužívání SW a multimédií stejně jako u běžných uživatelů, rozdíl je především ve větším objemu informačních technologií používaných jednotlivci využívající nelegální SW a multimédia pro komerční účely.

Dalším případem neoprávněného užívání SW bývá, když firma zakoupí menší počet licencí, než které skutečně užívá.

2.5.2 Výroba nelegálního SW

Také na našem trhu se vyskytuje nelegální padělaný SW (nejčastěji CD a DVD), zpravidla ho rozdělujeme na SW, který je vyráběn průmyslově a kopírování pro domácí účely.

2.5.2.1 Průmyslová výroba

K této výrobě pachatel potřebuje nějaké speciální vybavení nejčastěji továrního typu. Majitelé výrobních provozů se zabývají hlavně otázkou autorských práv. Musí se ověřit, zda si je zákazník oprávněn nechat si vyrobit konkrétní nosič obsahují SW či jiná data, toto ověřování bývá většinou složité. Může tedy nastat situace, kdy i renomovaný výrobce vyrobí spoustu datových nosičů s pirátským SW. Toto se nejčastěji stává při zadání výroby ze zahraničí, kam nakonec směřuje i hotový nosič s daty.

2.5.2.2 Domácí výroba

K uspokojení poptávky po nelegálním SW, či jiných datech dochází produkcí vytvářené hlavně v domácích podmínkách. Na tuto distribuci se podílí především velké množství

jednotlivců. Tyto jednotlivce, kteří vyrábí záznamová média popsaným způsobem můžeme celkem snadno odhalit a díky tomu se tato ilegální činnost daří celkem dobře potlačovat.

Hlavním důvodem padělání těchto dat je především jejich vysoká cena, která není dostupná pro všechny. Naproti tomu náklady na výrobu takovéhoto pirátského SW jsou zanedbatelné a zisky vysoké. Toto podněcuje spoustu lidí k výrobě těchto nelegálních dat.

2.5.2.3 Kopírovací služby

S rozvojem vypalovacích mechanik se zvýšil počet nabídek na kopírování dat. Tyto komerční služby byly v rozporu se zákonem, který byl často přehlížen nebo vědomě porušován. Kopírovaly se hlavně pirátské nosiče, či bylo vytvářeno větší množství záložních kopií, než bylo uvedeno v licenčních podmínkách, jenž byly dále poskytovány za poplatek, či zcela zdarma dalším uživatelům.

V dnešní době jsou tyto služby spíše minulostí, protože cena vypalovacích mechanik šla drasticky dolů a může si jí dovolit téměř každý.

Obrázek 8 autorské právo [20]

3 INFORMAČNÍ BEZPEČNOST

V dnešní době jsou informace velmi ceněným artiklem, a proto bychom měli dbát na informační bezpečnost s ohledem na rostoucí hodnotu informací v soukromém sektoru a v oblasti státní správy. Informace, které chceme chránit, mají různou podobu od písemné formy až po elektronickou. Riziko ztráty těchto informací hrozí jak zevnitř organizace, tak i mimo ní, a to právě pomocí počítače.

Informační bezpečnost je komplexní pohled, kterým si firma, či organizace chrání své cenné informace a také vede praktickým opatřením k eliminaci nebo významnému snížení dopadů v případě mimořádných událostí.

Definujeme ji jako zodpovědnost za informaci během vzniku, zpracování, přenosu, ukládání a likvidace.

Základními pravidly bezpečnosti informací jsou:

· **důvěrnost** (zajišťuje, že informace jsou přístupné pouze těm, kteří k ní mají

mít přístup),

· **dostupnost** (zajišťuje, že autorizovaní uživatelé mají k informacím v případě

potřeby vždy zajištěný přístup),

· **integrita** (zabezpečuje přesnost a úplnost informací a metod zpracování).

Obrázek 9 bezpečnost dat [19]

4 FORENZNÍ METODY

Obrázek 10 forenzní metody [18]

Forenzní metody ve výpočetní technice jsou speciální vědecké nástroje a postupy, které nám pomáhají při vyšetřování všech forem počítačové kriminality, či internímu šetření v organizaci.

Použití forenzních metod může představovat narušení fundamentálních práv občanů.

Proto zákonnost a následkem toho i přípustnost elektronických důkazů před soudem záleží, jak se respektují práva a povinnosti (omezení a záruky), ležící "vespod" legislativy vztahující se k informačním a komunikačním soukromí.

Podklady a procesní práva musí zajišťovat, že sbírka a pozdější jednání s nimi neporuší zaručení ochrany soukromých dat.

Článek 8 z evropské dohody a článek 7 ze základní listiny fundamentálních práv EU zaručující ochranu soukromí, proto zákonodárci musí upřesnit zákony a metody používání těchto dat.

Úměrnost, což je základní princip zákonů EU, vyžaduje další hodnocení odborníků v oboru, aby se našlo to nejlepší řešení a mohlo být dosaženo cíle.

Objektivnost musí být zaručena

Musí se zvážit závažnost zločinu oproti zločinu narušení soukromí a také se musí přizpůsobit zákonům všech zemí, protože každá má nějaké rozdíly

A) Technické překážky pro forenzní práce na iternetu

Zvýšená zločinnost v kyberprostoru se podepsala na zvyšující se potřebě rozvinutí a zdokonalení technik forenzního internetu a zařízení zabraňující útoku. Vyšetřovatelé, kteří

používají forenzní metody, by měli disponovat stejnými dovednostmi, jako jejich protivníci, hackeři. Vedle nezbytnosti vyšetřovatelů vyvinout a použít vhodné zařízení a postupy, aby mohli předvést digitální vyšetřování, stojí široká škála problémů, které je třeba vyřešit, což čítá technické, společenské, procesní a právní aspekty.

Procesní problémy vznikají z nedostatku standardizace, stejně jako z nedostatku teoretických struktur pro pole digitálních forenzních metod. Použití metod ad-hoc (konkrétních) a nástrojů pro vyzvědění digitálních důkazů může omezit spolehlivost a důvěryhodnost těchto nabytých dat, především v trestním řízení, kdy může být zpochybněn jak důkaz, tak metoda jeho získávání. Aby čelili tomuto problému, začali lidé z praxe, různá seskupení a organizace snažit vytvářet návrhy, jak standardizovat forenzní metody. Pro internetové forenzní metody je situace každopádně ještě složitější.

4.1 Forenzní analýza

Někdy přezdívaná jako ‘pitva systému‘ pro úzkou asociaci s chirurgickou prací, je to souhrn technik, nástrojů a postupů k **vyhledávání důkazů** na počítači, či počítačových systémech.

Tato analýza nám pomáhá určit, zda se skutečně jednalo o trestnou činnost, nebo vyvrátit daná obvinění.

Probíhá tam, kde je zapotřebí zkoumat počítačové systémy, či pouze data k ochraně, sběru a zhodnocení digitálních důkazů počítačové kriminality, porušení interních směrnic, krádeže duchovního vlastnictví, finanční podvody, poškozování síťových služeb organizace, nebo překročení pravomocí IT administrátorů, či uživatelů aj.

Hlavním cíl je tedy připravit všechny podklady pro další průběh vyšetřování počítačové kriminality. Snažíme se tedy určit to, co se stalo, kdy a jak se to stalo a kterých osob se to týká.

Tato věda spojuje velký okruh témat, a proto by jí měl provádět jen zkušený odborník, který musí mít velmi dobré znalosti v oblasti sítí, operačních systémů, HW, kryptografie aj., protože bez těchto znalostí, by nebyla taková analýza kompetentní a při neodborné manipulaci bychom mohli přijít ke ztrátě, či poškozením dat – důkazů.

Mimo to nám vyšetření deliktu zkušeným profesionálem může pomoci odhalit “skuliny“ v našem informačním systému a to může mít preventivní význam pro potencionální budoucí útoky na náš systém.

Výsledek forenzní počítačové analýzy slouží jako znalecký nebo technický posudek v soudním řízení, či v interním šetření organizace.

4.1.1 Forenzní analýza digitálních dat

Forenzní analýza digitálních dat je poměrně mladá věda, která původně zkoumala jen počítače, nyní se zabývá digitálními technologiemi ve všech směrech, tzn. počítači, datovými medii, mobilními telefony, mobilními sítěmi aj.

Můžeme jí tedy definovat jako užití vědeckých odvozených a osvědčených metod k ochraně, sběru, identifikaci, zhodnocení, analýze, transportu, dokumentaci, interpretaci a prezentaci digitálních dat, které jsou získány s digitálních zdrojů (hdd, cílových úložišť, aj.), k rekonstrukci podezřelých událostí, které by mohly vést až k trestné činnosti.

K analýze dat potřebujeme především původní sterilitu těchto digitálních dat (tzn., že zkoumaná data by měla zůstat v původní podobě nezměněny). Jestliže máme k dispozici dostatek času k vyšetřování, použijeme **forenzní duplikaci** zkoumaného média a tím vytvoříme kopii zkoumaných dat.

Pokud forenzní duplikaci nelze provést, je možné médium nastavit pouze ke čtení a nebyl na něj umožněn další zápis.

Takovéto informace – důkazy jsou obvykle skryty v podobě již smazaných dat, fragmentů dat v alokační paměti existujících souborů (slack space), v podobě tzv. logů (tzn. činností služeb, které běží na daném zařízení), nebo v již zmíněné dočasné paměti cash.

Data, které hledáme, se dělí do třech typů:

a) **aktivní** – jsou to sobory a adresáře, které jsou normálně viditelné a přístupné pro všechny uživatele a proto je nejsnadnější je získat
b) **archivovaná** – tyto data je možné nalézt na přenosných médiích typu CD, DVD, flash discích, aj.
c) **latentní** – tento typ dat bývá nejobtížnější získat, protože často představují již smazané, či částečně přepsané soubory. Získání těchto souborů bývá časově i finančně náročné a výsledek není zaručený. Navíc se může stát, že soubor může být ještě k tomu zašifrovaný a pak přichází na řadu kryptologové, kteří se snaží soubory dešifrovat, pokud je to možné. Někdy se může stát, že je šifrovací algoritmus příliš “silný“ a není k dispozici žádný dešifrovací klíč. Touto metodou se dá zašifrovat i celý cílový systém (např. Unix to umožňuje) a pak tedy zůstanou

všechny informace o datech vyšetřovatelům skryty. To ovšem platí jen, když byl daný počítač nástrojem zločinu. Pokud organizace šifruje data za účelem bezpečnosti, tak nemá důvod dešifrovací klíč policii nesdělit.

Dalším nezbytným úkolem je identifikace, nejprve si musíme určit, na kterých datových médiích by se mohly nacházet důležité informace pro naši analýzu. Samotné datové médium ale jako zdroj důkazů ještě nestačí, musíme vyextrahovat všechny informace, které považujeme za relevantní, a teprve potom **se stávají z těchto dat důkazy,** které dále musíme ještě roztřídit.

Nedílnou součástí forenzní analýzy dat je také interpretace informací, popřípadě důkazů. Správná interpretace může být zcela klíčová. Tyto informace si díky mnoha skriptům a GUI utilitám pro extrakci může obstarat téměř kdokoli, ale hlavní je jim porozumět a tedy je správně pochopit.

Ke správnému postupu patří jistě i dokumentace a proto bychom měli zaznamenávat všechny naše kroky od začátku až do konce, aby byla zřejmá posloupnost našeho postupu, protože u soudního řízení můžeme být dotazováni i na podrobnosti.

Vzhledem k tomu, že zadavatel analýzy nebo soud nebude znalý v oboru IT technologií, musíme umět prezentovat zjištěné skutečnosti vhodnou formou. Jde o to vystihnout podstatné zjištěné skutečnosti a zbytečně "nezabíhat" do technických podrobností, kterým by stejně nikdo nerozuměl (např. výpis logů aj.). Našemu zadavateli prostě sdělíme kdo je odpovědný za škody, nebo s jakými daty bylo manipulováno, či byly zcizeny.

Zkoumaný počítač může působit v roli nástroje zločinu, a nebo může vystupovat v roli oběti - tzn. v pozici, kdy je takový počítač nebo jiné zařízení terčem zločinu (například byla-li z takového počítače odcizena nějaká data, atd.). V takovém případě většinou uplatňujeme metody reakce na incidenty. V prvním případě, kdy je počítač nástrojem nějakého zneužívání nás jako výzkumníky, popř. vyšetřovatele nemůže překvapit, že zkoumané zařízení se nám do rukou dostane vypnuté nebo dostaneme prostě pouze média (disky, atd.) ke zkoumání. Takže nebudeme moci vytěžit informace z dočasné paměti RAM, běžíci procesy, sledovat síťová spojení, apod. Takové informace jsou však velmi důležité a často klíčové proto musí být metodologie reakce na incidenty (kterou využijeme v druhém případě, kdy je počítač v pozici oběti) postavena tak, aby byly tyto informace zachovány. [7]

4.1.2 Forenzní záchrana dat

Tato oblast patří k důležité a nedílné součásti v oblasti **forenzního vyšetřování. Záchrana dat** je široký pojem a předmětem záchrany dat se může stát jakékoliv přenosové médium, od diskových polí, přes flash disky, až po vypalovací média CD a DVD.

Prvním krokem této **obnovy dat** je diagnostika datového média, kde můžeme odhalit např. mechanickou závadu na zařízení, proto není vhodné pokračovat dále bez kopie dat tzv. **forenzní duplikace**, protože i samotné spuštění systému může přepsat původní uložená data.

Dalším důležitým faktorem této obnovy dat je použitý souborový systém (FAT, NTFS …), verze operačního systému a samotná aplikace, jenž pro uložení svých dat služeb tohoto systému využila.

Záchranu dat používáme v případě:

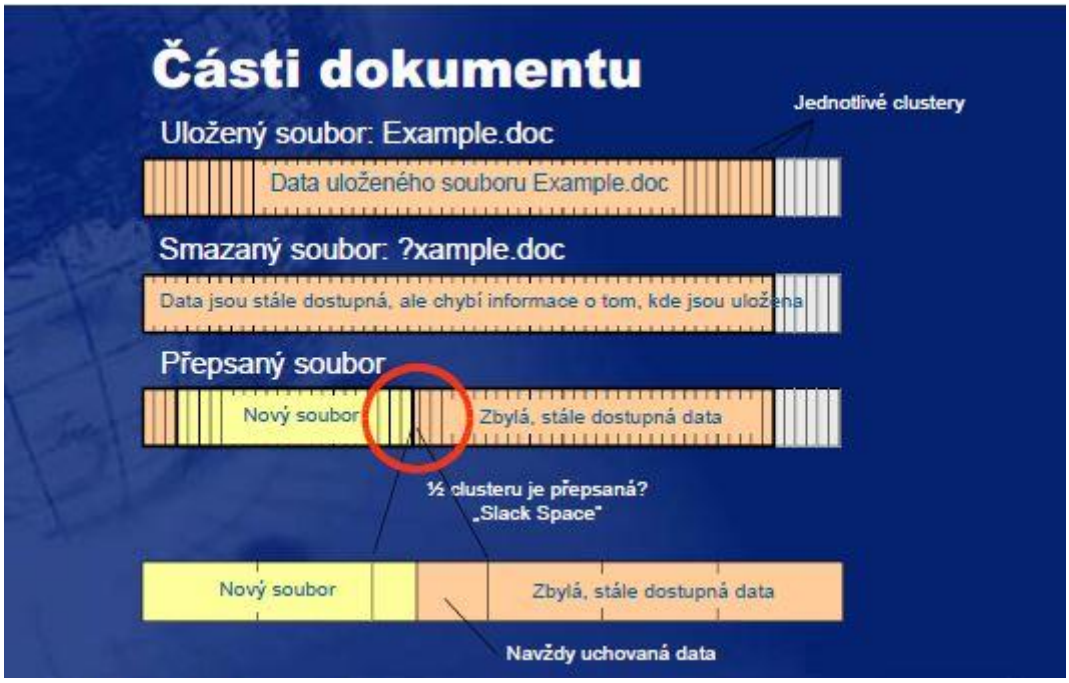
a) **chybí data –** SW problém
b) **data jsou nečitelná -** HW problém

Hlavním předpokladem je odbornost a vysoká interní znalost paměťových, souborových a operačních systémů, spíše z pohledu vývojáře. Jde především o to paměťové zařízení **zprovoznit** alespoň v laboratorních podmínkách, nebo takové data **odvodit** či **nahradit,** aby mohlo být obnoveno co největší možné množství dat.

Tímto způsobem můžeme řešit problém jen v případě, že je cílový paměťový disk nějak poškozen, či je opotřebením snížena jeho funkce. Může se stát, že data byla smazána záměrně a proto se využijeme další forenzní nástroj – **forenzní audit,** který zkoumá všechny stopy (nejen digitální).

Tento postup je ale téměř nemožný bez speciálních programů, protože osoba, která se dopouští tohoto protiprávního jednání si je toho z pravidla dobře vědoma a snaží se po sobě všechny "**kyberstopy zahladit**", to ale odpovídá míře znalosti výpočetní techniky.

Pachatel se může pokusit **zbavit stop** SW (odstraněním z cash, fyzické paměti aj.), nebo HW (fyzická likvidace disku, založení požáru …), ale ani tato likvidace důkazů není s použitím speciálních nástrojů jistá, v opačném případě může nastat tato situace



Obrázek 11 forenzní metoda záchrany dat [4]

Při **záchraně dat** je vždy cílem obnovit obsah, formát i kontext dat v maximální možné míře. Při **forenzním auditu** ale často postačí prokázat nebo nalézt pouze kontext, kontext a fragmenty obsahu nebo pouze fragmenty obsahu. Podobá se to policejní práci, kdy podezřelý může jen obtížně tvrdit, že oběť neznal, když má ve svém mobilu uloženo její číslo a v kalendáři záznam o schůzce. Obdobně při počítačovém forenzním auditu hledáme, zda se na počítači nebo jiném zařízení pro zpracování dat vyskytl nějaký dokument, byla nějaká data vytištěna, exportována, odeslána nebo přijata a to například s ohledem na výskyt textu, který charakterizuje prošetřované podezření. (4)

4.1.3 Forenzní duplikace

Další z forenzních nástrojů je tzv. **forenzní duplikace.** Tuto zálohu je vhodné použít pro pozdější analýzu, tedy pokud je to technicky možné a máme na to v průběhu vyšetřování dostatek času.

Duplikaci provádíme hlavně proto, aby se nenarušila původní data a tak bychom přišli o původní důkazní materiál (např. přepsání přístupových časů k souborům).

Používáme opět jen speciálního SW od jednoduchých unixových programů, až po sofistikované komerční nástroje mající celou škálu různých funkcí.

Vytváření duplikací terabytových disků může být časově i finančně velice náročné a proto organizace nemusí mít dostatek času a prostředků, navíc v době kdy došlo k incidentu.

Musíme tedy uvážit, zda-li je taková duplikace celých systémů vůbec nutná a jestli je incident natolik vážný, abychom vynaložili takové úsilí a prostředky k získání důkazů.

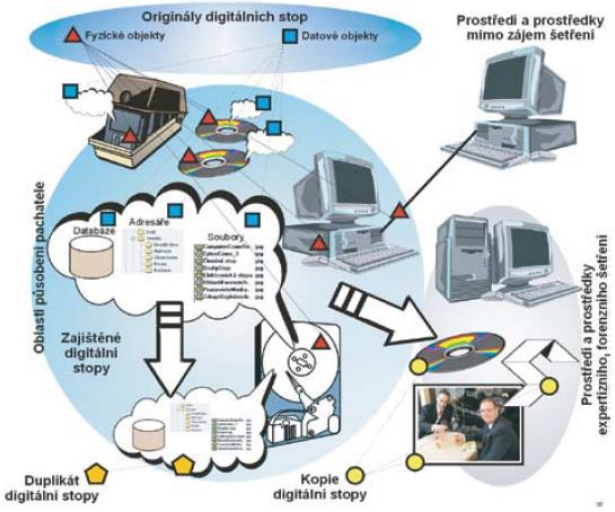
Z tohoto důvodu provádíme jen tzv. logickou kopii (zkopírování např. aplikačních a systémových logů, duplikace odstraněných oddílů aj.).

4.1.3.1 Duplikát

Jedná se o přesnou repliku digitálního datového média, které se ukládá na stejný typ datového uložiště v poměru 1:1 včetně všech jeho fyzických i logických vazeb. Duplikace se vytváří hlavně kvůli zachování původních dat, protože tyto data mohou být později ještě přezkoumány jinými nezávislými znalci, nebo na ně mohou být aplikovány jiné postupy a metody. Nevýhodou duplikací je, že se musí rekonstruovat včetně všech skrytých vazeb a mohou mít tedy obrovský objem dat.

4.1.3.2 Kopie

Je to reprodukce datových médií z původního fyzického objektu na jiný nezávislý typ. Na rozdíl od duplikátu nekopírujeme vše, ale vybíráme jen taková data, která jsou pro nás relevantní pro další zkoumání. Při kopírování ale mohou být narušeny funkční a logické vazby s dalšími datovými objekty a tyto kopie tedy nemusí jako důkaz vůbec stačit, protože nemusíme mít k dispozici všechna data, která jsou nezbytná k vyšetřování. Proto je při forenzním šetření je vhodné mít k dispozici originál, či jejich duplikát.



Obrázek 12 ukládání digitálních stop [3]

4.1.4 Forenzní audit

Prokázáním účetních podvodů, zpronevěr a jiných protiprávních činů se zabývá **forenzní audit** a spočívá k prověřování finančních, obchodních dokumentů, účetních závěrek a záznamů, či výročních zpráv subjektu. Prozkoumává i data, která nemusela mít přímou souvislost s tímto trestným činem (chaty (diskuzní fóra), elektronickou poštu, tabulky, fyzické dokumenty, aj.).

Protože při **forenzním auditu** nepracujeme jen s obnovou digitálních dat, ale metody nashromáždění informací se provádějí komplexněji, pracujeme i s daty, co nebyla nikterak skryta. S daty, která jsou bez poškození, zálohy, archivy také se skenují i fyzické papírové dokumenty. Tyto data jsou dále "vyčištěna", indexována a identifikována, což umožní jejich důkladnější rozbor a pomůže nalézt vše, co se týká konkrétního obchodního případu.

Forenzní laboratoře pro speciální postupy jsou vybaveny mnoha specializovanými zařízeními, na kterých pracují odborníci, kteří dokáží nalézt, či rekonstruovat data, které mohou hrát klíčovou roli v objasnění určitého případu, ale ani to nedává jistotu bezchybné práce vzhledem k obtížnosti úkonu, kterým tato forenzní metoda bezesporu je, proto je právní a technická konzultace vždy na prvním místě a u soudu není tato metoda brána v potaz jako plně průkazný důkazní materiál.

Obrázek 13 forenzní audit [4]

4.1.5 Forenzní analýza síťového prostředí

Existuje odhad, podle kterého je na světě asi 300 miliónů lidí, kteří již použili internet. Z tohoto počtu se dále odhaduje, že asi 5 procent nemělo zcela čisté úmysly, a kdyby jen desetina lidí byla zkušená v oblasti IT, dělá nám to asi **1,5 mil. potencionálních útočníků**.

Proto musíme brát v potaz, že data se nepřenáší jen po externích přenosných médiích, ale hlavní přenos informací probíhá přes počítačovou síť, proto si musíme být vědomi toho, že hlavní ohrožení číhá právě tam. Právě přes síť se k nám může dostat různá počítačová "havěť" (viry, trojské koně, červi a individuální útoky) a nesmíme zapomenout na šíření ilegálních programů, či materiálů.

Při vyšetřovat neoprávněných, či ilegálních aktivit je potřeba shromažďovat důkazy z akcí při provozu sítě. Musíme tedy pečlivě sledovat síťový provoz a výsledky provozu zaznamenávat do tzv. logů pro další rozbor.

Jestliže logujeme síť pravidelně, můžeme detekovat zakázanou akci, ještě před její plném uskutečněním, k tomu ale potřebujeme mít vysokou znalost provozu sítě, zejména síťového protokolu TCP/IP, včetně jeho služeb a aplikací.

Kvůli těmto potřebám logování sítě a rekonstrukci paketů, vznikly **speciální nástroje:**

a) **sniffery**: nástroje pro zachytávání síťového provozu, které jsou často zneužívány počítačovými hackery k nezákonné činnosti. Často bývají částí IDS (Intrusion Detection System) a tvoří zde více komplexní nástroj k detekci sofistikovanějšího typu průniků do sítě.
b) **nástroj pro rekonstrukci paketů:** dokáží znovu rekonstruovat do původního stavu zachycené pakety, nebo jen jejich fragmenty.

Účelem těchto nástrojů je především **detekce incidentu**, identifikace a následná **eliminace škod.** Samozřejmě je lze využít ke sběru důkazního materiálu, který může pomoci potvrdit, či vyvrátit nežádoucí činnost jak zaměstnance, tak i účastníka síťového provozu.

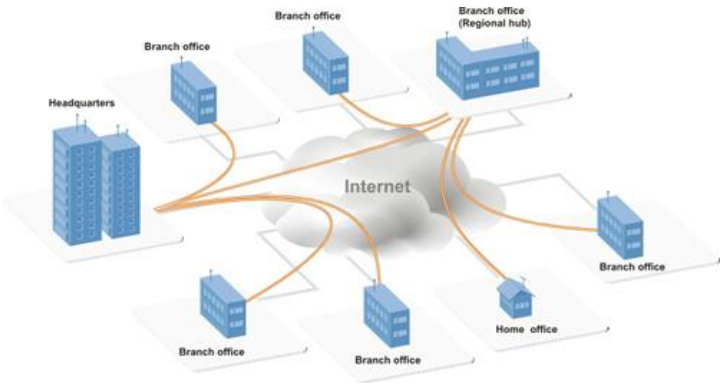
Jako je každý člověk jedinečný a má svůj určující znak, nezaměnitelný s jiným, tak i počítače zanechávají po sobě **stopy v podobě např. IP adresy**. Můžeme tedy získat tzv. síťové důkazy, jenž obsahují informace o daných skutečnostech v síti na konkrétním PC.

Tyto informace se ale vždy netýkají jen prozkoumávaného počítače. Sítě jsou rozmanité a jsou tvořeny i dalšími sítovými prvky (routery, směrovače, firewally, aj.), které nám mohou být cenným zdrojem informací o provozu na síti a tedy i na jednotlivých PC. Tyto

prvky mohou obsahovat nástroj IDS, který je určen především k logování sítě a detekci podezřelých aktivit.

Samotná orientace v těchto informacích může být extrémně složitá, protože jednotlivé logy nemusí být ve stejném formátu, navíc záznamy nemusí být ani ve stejném časovém pásmu, což může způsobit ještě větší chaos.

Dalším problémem vyšetřovatelů může být, že logy které mají k dispozici mohou být již upraveny, protože útočníci často užívají tzv. čističe logů a tudíž neodpovídají skutečnému síťovému provozu.



Obrázek 14 počítačová síť [10]

4.1.6 Forenzní analýza mobilních telefonů

Jako lidé mají svůj specifický znak v podobě otisku prstu, počítač svou IP adresu, tak i mobilní telefony obsahují data v podobě zpráv SMS, fotografií, sítě kontaktů, historie telefonu, dat ze sociálních sítí e-mailů aj, které mohou zařízení jednoznačně identifikovat.

Vzhledem k obrovskému vývoji mobilních aplikací může uživatel ukládat své data jak na internet, tak i lokálně do telefonu a proto můžeme zjistit mnohem více informací než dříve.

K výpisu hovorů se můžeme obrátit na poskytovatele služeb, ale jen v případě, že dostaneme soudní příkaz, který může být obstarat velmi časově náročné a právě čas hraje často klíčovou roli v průběhu vyšetřování, navíc se může stát, že daný operátor sídlí v zahraničí, přitom **forenzní analýza telefonu** je velmi efektivní k prověření podezřelých osob, nebo na místech kdy je telefon jediným zdrojem informací.

Využitím moderních nástrojů můžeme rychle a efektivně **vyextrahovat potřebné informace a ihned jednat.** Jestliže neprovádíme nějakou nezákonnou činnost, tak nám mobilní telefon může být užitečný v mnoha směrech.

V opačném případě se může stát takovýto mobil cenným **zdrojem důkazů**. Ale i samotná komunikace pro zločince může být bezpečná, protože se dá velmi efektivně **šifrovat**. Právě proto je velmi důležité mít potřebný um vyextrahovat data z takového mobilního telefonu, která nám mohou pomoci usvědčit pachatele

4.1.6.1 Nástroje pro forenzní analýzu mobilních telefonů

V podstatě existují 2 typy nástrojů k provedení forenzní analýzy mobilních telefonů, každý z těchto typů má své výhody a nevýhody.

a) **Hardwarové:** tyto analyzátory pracují samostatně, ale slouží jen ke sběru dat, k následné analýze dat je zapotřebí ještě počítač se speciálním SW. Jejich předností je mobilita, naopak jejich nevýhoda je vysoká pořizovací cena. Asi nejvýznamnější nástroj je UFED od izraelské firmy Cellebrite.
b) **Softwarové:** naproti tomu jsou tyto analyzátory levnější než HW a jen uživatel si sám zvolí, na který typ počítače si danou aplikaci nainstaluje. Uživatel může upřednostňovat výkon nebo mobilitu a tím mu vzniká větší komfort. Mezi přední SW nástroj je český MOBILedit Forensis.

Zisk a analýza klíčových dat už se sice nedělá manuálně jako dříve, ale to neznamená, že dnes je tato práce mnohem jednoduší, je to způsobeno především absencí standardizovaného komunikačního protokolu, každý výrobce používá svůj vlastní.

Samotný vývoj takového nástroje je velice obtížný, poněvadž každý telefonní přístroj je svým způsoben jedinečný, navíc i stejný telefon může mít jinou verzi firmwaru (Firmware je malý softwarový program, který řídí funkce a činnost produktů řízených mikročipovým procesorem) a samotný výrobce nemá své komunikační protokoly řádně zdokumentované.

Z tohoto důvodu vznikají různé platformy především pro telefony firmy Apple (iPhone) a mobilní telefony používající OS Android, protože tyto telefony obsahují největší objem dat.

Je potřeba mít na paměti, že tuto analýzu neprovádíme jen pro nejmodernější telefony, které jsou na trhu k dispozici, ale zkoumáme i starší typy mobilů, protože i tyto přístroje lidé stále používají, takže by měl být takový nástroj více komplexnější.

4.1.6.2 Situace v ČR

U nás je tato metoda využívána již řadu let a z celosvětového hlediska patří mezi špičky na celém světě. Postupem času se forenzní analýza mobilních telefonů začala stejně jako forenzní analýza počítače využívat při soudním řízení. Soudy postupem času "vstřebávají" tyto nové technologie a postupně se učí využívat tyto důkazy.

Překážkou v tomto progresu je přílišná nekompetentnost představitelů soudnictví, kteří nedokáží včas reagovat na enormní vývoj těchto technologií. Proto je důležitou částí vzdělávání představitelů soudu a dalších odborníků.

Obrázek 15 mobil [15]

5 ZPŮSOBY VYHLEDÁVÁNÍ VIRŮ

5.1 Virová databáze

Je to vlastně seznam již existujících virů a jejich zdrojových kódů, které viry obsahují, popřípadě dat o virech. Systém potom skenuje data v počítači a porovnává je s databází. Každá databáze obsahuje datum aktuální verze, a proto musí být pravidelně aktualizován, kvůli aktuálnosti virů a jejich zdrojových kódů. Každá neaktualizovaná databáze představuje bezpečnostní riziko z důvodů nových nebo aktualizovaných virů, které již nejsou zahrnuty v neaktualizované databázi.

Informace, na jejichž základě lze jednotlivé viry identifikovat:

A) **Signatury:** tj. sekvence znaků, které se vyskytují v těle (zdrojových kódech) jednotlivých počítačových virů, případně zjistitelné kontrolním součtem.

B**) Kontrolní součty CRC statických částí viru:** snižuje riziko falešných poplachů, které způsobuje náhodné výskyty v „těle“ zdravého programu. Od tohoto součtu lze odhalit celé rodiny daného viru.

Každá antivirová společnost má svou virovou databázi a různý počet antivirových databází zdrojových kódů různých virů. Každá databáze je svým způsobem jedinečná. Od této databáze se nedá určit kvalita antivirového programu. Velice těžko se také určuje, zda-li je lepší antivirová databáze, která se aktualizuje např. každý den nebo každých 12 hodin. Podle mého názoru je nejlepší taková databáze, která je schopna zareagovat na virovou hrozbu co nejdříve od jejího vzniku.

5.2 Dynamická emulace kódu

Touto technikou se vyhledávají především složitější viry. Je to způsob proměnlivé diagnostiky pro nejsložitější typy infiltrací, jež jsou zakódované různými modifikovanými způsoby, které pak nemůžeme najít podle statických signatur, a proto musíme použít dynamické emulátory kódu. Jsou to obsáhlé detekční metody, které simulují spuštění a průběh procesu v počítači (simulace procesoru). Asi největším plusem je, že touto technikou nemůžeme nijak ohrozit náš počítač a simulace nám ukáže “vývoj“ takového dynamického viru až do podoby statické, kdy ho můžeme detekovat na základě statických signatur. Vyskytují se i některé antivirové programy, které obsahují kompletní takovéto skripty, díky kterým můžeme detekovat i zaheslované skriptové viry.

5.3 Kontrola integrity dat

CRC checker porovnává aktuální stav zvolených nebo určených programů, různých particion (část diskové jednotky) na disku, které byly uloženy ještě dříve nebo při instalaci kontrolním programem. Jakmile se virus dostane do takto kontrolovaných souborů, kontrolovaný objekt na sebe poté upozorní a virus je odhalen. Virus se může přichytit za tělo, před tělo i do těla programu. Výhodou tohoto způsobu vyhledávání je, že jsme schopni najít i nové a ještě nedetekované a dosud neznáme druhy virů, které zatím ještě nemůžeme nijak skenovat a neúčinná je i heuristická analýza. Ne vždy se dá kontrolou integrity uspět a to zejména u starších programů, které svou konfiguraci ještě zapisují do EXE souboru, sice je zkontrolovat můžeme, ale je téměř nemožné odlišit jejich chování od infikace virem. Náš kontrolní program zobrazuje varovné protokoly, ale v takovýchto situacích záleží jen a pouze na znalostech daného uživatele.

5.3.1 Místa útoků virů

a) **Prepend** – virus se "přichytí" před samotný program

b) **Append** – virus se umístí za samotný program

c) **Insert** – virus se umístí do samotného těla programu

S informacemi o souboru může tento program pro kontrolu integrity dat odstranit takovýto virus bez znalostí dalších informací i "díky" kontrolnímu součtu souborů, který si taková kontrola integrity z detekčních důvodů pamatuje i díky tomu pozná zda-li byl pokus o odstranění takového viru úspěšný. Tento způsob z tohoto důvodu patří k nejbezpečnějším vůbec. Nevýhodou uvedeného způsobu je, že kontrola integrity dat musí být provedena ještě před zavirováním počítače, protože když označíme soubory, které jsou již zavirované, tato kontrola je bere za bezpečné. Těchto programů na kontrolu integrity však v poslední době rapidně ubývá a většinou jsou spojeny s "on-deamond skenerem" z jasného důvodu, a to je „pohodlí" uživatelů. Uživatel si nechce sám stahovat programy na diagnostiku, filtrování a antivirový program pro konkrétní virové ohrožení, ale raději si obstará jeden kompletní program, který obsahuje všechny tyto již zmíněné prvky.

5.4 Genetická detekce

Je to nejednoduší způsob, jak nalézt daný virus. Předpoklad je, že daný virus má již svého předchůdce a tzn., že vznikl pomocí „mutace“ z jiného „příbuzného“ viru. Tímto způsobem funguje i generický scanner, který obsahuje základní databázi druhů již rozpoznaných signatur, díky které můžeme snadno a bezpečně poznat takovýto „příbuzný“ virus daného druhu. Tento generický scanner prohledává místa na disku a porovnává data již se známými signaturami.

5.5 Heuristická analýza

Je to další typ virového vyhledávání. V současné době je to asi vůbec nejrozšířenější nástroj k odhalení virové infiltrace, který obsahuje celá škála u antivirových programů. Test trvá sice déle, jak normální virový scan, ale zase je mnohem důkladnější. Hlavní jeho princip je založen na schopnosti “porozumnění“ kódu programu na straně antiviru, ten logicky vyhodnotí kód testovaného objektu a dále se simuluje, co testovaný kód znamená v praxi a na jeho základě vše vyhodnotí (tzn. infikován/ bez viru). Hlavní výhodou je možnost detekovat dosud ještě neznámé viry. Velkou nevýhodou této analýzy bývalo velké množství falešných poplachů, ale v poslední době se jejich výskyt omezil takřka na minimum.

A) Statická heuristická analýza: Je to součást heuristické analýzy a doplňuje dynamickou analýzu. Provádí prvotní ohledání podezřelého shluku zdrojových kódů a dalších podezřelých aktivit (flags) ještě před emulací. To nám pomáhá hlavně při dalším stanovení následujícího postupu. Tento nástroj nepoužívá signatury, ale vyhledává spíše obecné podezření infiltrace, čímž může detekovat i dosud neznámé viry, které dosud nejsou v žádné virové databázi. Nevýhodou je, že tato metoda nepronikne “pod povrch“ těchto polymorfních či zaheslovaných virů a složitější viry tedy nedokáže rozpoznat.

B) Dynamická heuristická analýza: Je to jedna z nejspolehlivější zbraní proti útokům neznámých virů. Tato analýza hledá hlavně konstrukci typickou pro počítačový virus. Základním “kamenem“ je emulátor virtuálního prostředí počítače. Tzn., že tento nástroj virtuálně od-emuluje takovýto soubor jako by ho přímo spustil uživatel počítače. V tomto prostředí daný virus nemůže počítač nijak ohrozit, ale můžeme sledovat jeho další případný “ vývoj“, jako by byl soubor infikován a daný emulátor (dekryptor) provádí

simulovaně činnost daného viru, který ho v takovém stavu již snadno může detekovat virovým skenerem a virus je následně odhalen.

C) Run-time heuristická analýza: Je to vlastně analýza, která běží v reálném čase. Tato analýza analyzuje obsah, který se vyhodnocuje v průběhu běžící kontroly disku nebo konkrétních souborů. Před samotnou kontrolou statickou či dynamickou se nás tento nástroj táže, zda jsme již soubory, které chceme zkontrolovat, již dříve run-timově testovali. V případě, že ano, tak záleží na množství stanovených výskytů. Když tyto výskyty přesáhnou stanovený limit, jsou vyhodnoceny jako podezřelé. Tato technika se doporučuje na poštovních serverech, kde může včasně zabránit následné virové epidemii, ale už méně se doporučuje ke kontrole celých diskových polí z důvodu citelného zpomalení systému.

5.6 Rezidentní štít

Většinou se jedná o část antivirového programu, který se hned po startu počítače zavede do operační paměti, kde potom kontroluje všechny, či zvolené soubory a e-maily. Jestliže "narazí" na virus informuje o tom uživatele ještě před tím, než se soubor spustí. Efektivita a rychlost je vysoká, a tak je velmi nepravděpodobné, aby se do systému dostal již známý virus.

5.7 Sandbox

Tam kde emulátor nestačí simulovat celý běh operačního systému, je třeba použít sandbox. Sandbox sice není přímo nástroj určený k detekci, ale může nám pomoci k otevření neověřených e-mailů a příloh od 3. strany. Umožňuje pomocí virtuálního prostředí, které je plně odděleno od operačního systému, otevřít potencionálně nebezpečný software, aniž by hrozilo nějaké nebezpečí virové nákazy. K dalším možnostem sandboxu patří i otevírání e-mailových příloh, a tak sandbox zabraňuje infiltraci jak viry, tak spywarem a dalším nebezpečným softwarem. Sandbox je poměrně nová metoda a vyskytuje se ve formě serverů, či specializovaných programů. Celý proces probíhá v simulovaném chráněném prostředí, kam nemůže vniknout žádný virus. Virus nemůže nijak zjistit, že se nachází v takovémto prostředí a tak pracuje, "jak by měl". Díky tomu můžeme podrobněji analyzovat všechny činnosti takového viru. Následně jsou všechny tyto činnosti vyhodnoceny a systém se kompletně obnoví. (všechny modifikované a zavirované soubory zanikají).

6 ZÁKLADNÍ DĚLENÍ VIRŮ

Obrázek 16 viry [16]

6.1 Dle oblasti napadení

A) **Boot viry**: Jedná se o nejstarší skupinu virů, které se nacházejí ve vyhraněných částech disku (boot (zaváděcí část disku) sektory a MBR) a tím mají zajištěnu svou aktivaci hned po spuštění systému. Viry obvykle přepíší svým tělem boot sektor a původní boot část umístí jinam na disk. Nebezpečí hrozí když virus infikuje nějakou kritickou část systém (FAT ..), a tak může dojít ke ztrátě dat. Nejčastěji se šíří pomocí disket a jiných přenosných medií.

B) **Soubor ové viry**: Jejich cíl infikace je samotný soubor. Můžeme je dělit podle toho, jaký typ cílových souborů napadají. Virus se snaží o to, aby se co nejvíce šířil. Postup všech cílů je podobný a jsou to:

1) spustitelné soubory s příponou (COM, EXE ...)

2) dávkové soubory BAT

3) systémové ovladače SYS

C) **Multiparitní viry**: Kombinují způsoby šíření boot virů a souborových virů. Mohou infikovat jak particion tabulku na pevném disku, ale i tak spustitelné soubory typu EXE, COM, aj.. Virus musí vyčkat na dokončení zavádění operačního systému a poté převezme kontrolu "vyšší úrovně" služeb dosu.

D) **Makroviry:** Již z názvu je znatelné, že makroviry jsou tvořeny z maker (aplikace k zjednodušení práce např. klávesová makra). Takové makro, které dokáže opakovaně zkopírovat své tělo z jednoho dokumentu do druhého nazýváme makrovirem. K úspěšnému šíření je zapotřebí, aby daná aplikace bylo hodně používaná. Dochází tím k výměně dat mezi jednotlivými uživateli v počítači. Všechny tyto podmínky splňují programy od Microsoftu (Word, Excel ...) a "díky" tomu se právě přes tyto programy makroviry nejvíce šíří. Virus je uložen v dokumentu, a když je otevřen a načten danou aplikací, může se za určitých podmínek aktivovat (pomocí automaker) a tedy i dál šířit do všech nově vytvořených, modifikovaných, či jenom otevřených dokumentů.

6.2 Základní typy nezákonných infiltrací

A) **Počítačové viry**: Název je odvozen od virů biologických, které se šíří dál z člověka na člověka. Počítačový virus se dokáže sebereplikovat a šířit ze souboru na soubor a také se dále šířit. Některé viry mohou i narušovat bezpečnost počítače, kdy "sbírají" údaje a důležité informace (hesla, emailové adresy …), které odesílají zpět k původci viru nebo na předem určené místo.

B) **Červi**: Tento vir nenapadá žádné soubory, ale šíří dál sám sebe pomocí e-mailové pošty přílohou, nebo podobným způsobem. Napadá pouze jeden program (sadu souborů) na hostitelském počítači a využívá jeho komunikační možnosti propojení s dalšími počítači. Virus není součástí žádných hostitelských souborů, ani se dál nešíří lokálně.

C) **Trojský kůň**: Virus se navenek chová jako regulérní program a plní svou funkci (spořič obrazovky, hra, antivirový software ...). Tato činnost ale pouze maskuje jeho pravou funkci. Uživatel neví to, že tím umožňuje přístup nežádaným uživatelům do PC.

D) **Backdoor**: Aplikace typu klient-server kdy umožňuje útočníkovi obejít autentizaci uživatelů a zároveň zůstat skrytý před běžnou kontrolou při aktivaci do systému. Má formu samostatného programu nebo je jeho modifikací. Vstup do systému probíhá fiktivním zadáním uživatele a hesla, kterým má pak volný přístup do systému jako administrátor. Útočník tím může vzdáleně přistupovat do počítače dle své libosti.

E) **Spyware**: Je to nástroj pro cílenou reklamu. Tento program využívá internetu k odesílání dat bez vědomí uživatele jako klasický backdoor, ale s tím rozdílem, že posílá pouze statistická data (navštívené www stránky, používané programy ...). Často se šíří společně s sharewarovými programy, o jejichž existenci autoři často vědí.

F) **Adware**: Tento produkt obvykle znepříjemňuje práci s reklamou (“vyskakující“ okna POP-UP). Cíl takové aplikace je “ vnucování“ nějakého produktu, aplikace, či www stránek, o které uživatel nemá zájem.

G) **Hoax**: Jde o neexistující poplašnou zprávu, která obvykle varuje před neexistujícím nebezpečím. Šíření závisí hlavně na uživatelích, kteří takovouto zprávu obdrží na svůj mail a chtějí varovat své známé a tím vzniká celý koloběh šíření.

H) **Cybersquatting:** Jde o zkupování známých domén, které si vlastník zaregistruje sám na sebe jako internetové adresy s cílem prodeje s velkým ziskem bohatým společnostem, které chtějí danou doménu vlastnit. V posledních letech je cybersqatting na vzestupu a má vzrůstající tendenci.

Vedle této metody existuje nová forma, která se nazývá Typosquatting. Je to rozvinutější forma cybersquattingu a využívá předvídání překlepů při ruční zadávání adresy, proto se velké firmy snaží, zkoupit adresy i s možnými překlepy.

Typický příklad v ČR je www.facebook.cz namísto com, kde se místo sociální sítě facebooku spustí vlezlá reklama.

CH) **Dialer**: Tato hrozba byla aktuální spíše u připojení typu dial-up, kdy infikovaný soubor změnil číslo poskytovatele připojení a tím změnil i tarif za danou službu. U infikovaného počítače byl obvykle vypnut reproduktor a uživatel byl přepojen na tuto službu v řádech mnohem vyšší ceny. Na počítač se obvykle dostane “díky“ technologii ActiveX.

I) **Phishing**: Podvodná metoda využívající internetu, e-mailové pošty a sociálního inženýrství, kdy se pod hlavičkou seriózní společnosti snaží z uživatele vylákat citlivé informace (hesla, rodná čísla, čísla kreditních karet, aj.), proto doporučuji vždy pořádně kontrolovat, od koho je vlastně tento e- mail a své citlivé informace posílat jen věruhodným a prověřeným adresátům v zabezpečeném režimu (např. https).

J) **Pharming**: Je to nástupce phishingu někdy nazýváno farmaření, jenž se snaží ukrást citlivá data oběti. Napadá DNS (server s doménou) a přepíše IP adresy, což klienta přesměruje např. na fiktivní stránky internetbankingu, které jsou od nerozeznání od originálu.

Obrázek 17 počítačová kriminalita [17]

V této části jsme si popsali historii počítačové kriminality, virologii, různé formy páchání nezákonné činosti spolu s typickými trestnými činy. Definovali jsme si pojem informační bezpečnost a nastínili forenzní metody, které nám slouží ke zkoumání digitálních důkazů.

V následující praktické části si **na našem fiktivním případu zločinu prakticky ukážeme**, jak postupují vyšetřovatelé na místě činu a jakým způsobem celou situaci vyšetřují. Dále si nastíníme postupy a rozbory, které se provádí ve forenzních laboratořích.

II. PRAKTICKÁ ČÁST

7 VYŠETŘOVÁNÍ NEZÁKONNÉ ČINNOSTI V OBLASTI VÝPOČETNÍ TECHNIKY

K vyšetřování nezákonné činnosti v této oblasti je potřeba skloubit více vědních oborů a metod, především forenzní a kriminalistické metody. Protože je toto odvětví svým způsobem specifické a velmi rozsáhlé je potřeba rozčlenit práci na kriminalistickou, kde se provedou všechny nezbytné kriminalistické metody (zajištění stop, identifikace, výslech všech podezřelých, výpis hovorů, aj.) a forenzní metody (vyhledávání, analýza digitálních dat, dupĺikace dat, analýza síťových prostředků aj.).

K těmto postupům je zapotřebí zejména vysoká odbornost v daném oboru, a proto je kladen velký důraz na spolupráci vyšetřovatelů a expertů v oblasti výpočetní techniky, kteří mají k dispozici mnoho nástrojů, jenž napomáhají k získávání digitálních stop.

Počítačová kriminalita je trestný čin, který je páchán proti výpočetní technice, datům a programovému vybavení, která je také využívána jako forma kterékoliv trestné činnosti.

Obrázek 18 oblasti vyšetřování počítačové kriminality [13]

7.1 Právní aspekty k vyšetřování počítačové kriminality

K provedení forenzní analýzy je zapotřebí získat nějaký zdroj dat, jenž zajišťují kriminalisté různými způsoby. Zde si rozdělíme zásady zajišťování dat pro potřeby trestního řízení.

V průběhu trestního řízení zajišťují orgány činné v trestním řízení hlavně tyto úkony:

1) ohledání a zajištění místa činu, které je klíčové pro další vyšetřování
2) osobní, či domovní prohlídku
3) vydání, či odnětí věci
4) prohlídku jiných prostorů
5) kontrolní nákup ve spolupráci s ČOI
6) a další

7.1.1 Dokazování v trestném řízení

Pro úspěšné posouzení vyšetřovaného skutku je nezbytné nejprve správně určit okolnosti, tedy stanovíme rozsah a obsah předmětu dokazování. Musíme také zabezpečit objektivnost, úplnost a rychlost.

Dle zákonného ustanovení **§ 89 odst. 1 trestního řádu** je nezbytné dokazovat především:

- jestli se skutek, v němž je podezření z nezákonné činnosti, skutečně stal
- zda-li je obviněný skutečně odpovědný za nezákonné jednání, popřípadě za jakých skutečností
- další okolnosti, které mají posouzení nebezpečnosti činu
- okolností z osobních poměrů pachatele
- skutečnosti vedoucí nebo k umožnění spáchat trestnou činnost
- okolnosti stanovující následky a výši způsobených škod trestným činem

7.2 Příprava a zajištění stop

Oblast výpočetní techniky zahrnuje celou škálu různých technologií, a proto je téměř nemožné zajistit specialistu, který plně ovládá všechny druhy systémů, všechny technologie a všechny druhy forenzních postupů zkoumání. Je-li to možné, zjistíme alespoň některé informace o problematice incidentu předem. Snažíme se zjistit počty a druhy počítačů, druhy programového vybavení, druh OS, specifika síťového provozu, zda-li bylo použito šifrování, odbornost personálu popřípadě informace o struktuře objektu. Za předpokladu, že organizace používá hesla nebo šifruje data, je dobré využít kriminalistickou operativní činnost (k zjištění tajného klíče), která nám může práci velmi urychlit.

7.2.1 Ohledání místa činu

Za místo činu se považuje prostor nebo část prostoru, o kterém se domníváme, že podle jeho vnějších znaků se dá usuzovat, že na tomto místě byl **spáchán či bylo napomoženo spáchání trestného činu.**

Je to specifická kriminalistická disciplína, kterou na základě přímého pozorování zkoumá, hodnotí a vystihuje materiální stav místa, který má bezprostřední vztah ke zkoumané události, za účelem identifikace a získávání stop a dalšího důležitého materiálu k dalšímu vyšetřování.

Tento úkon najdeme v trestním řádu v **zák. č. 141/1961 Sb**. Je jedním z nejdůležitějších druhů ohledání, který má své specifika jako je neodkladnost, neopakovatelnost a nezastupitelnost a provádíme ho dle stanovených zásad.

O všech provedených úkonech sepisujeme písemný protokol, jenž popisuje celý průběh ohledání místa činu.

7.2.1.1 Postup na místě činu

Základní rozdělení místa činu, kde údajně došlo ke spáchání trestné činnosti je:

A) **Materiální místo činu:** Na tomto místě měl být spáchán trestný čin nebo se na něm projevily účinky trestného činu. Zde nás nezajímají digitální data (stopy), ale zaměřujeme se zde především na vše hmatatelné, což může být např. diář, poznámky, odpadkový koš, nástěnka, otisky prstů, apod.

Obrázek 19 stopy na místě činu [13]

B) **Digitální místo činu:** Zde neprovádíme žádné další **forenzní zkoumání**, musíme především dbát na to, aby bylo **místo činu řádně zabezpečeno** a nikdo nemohl manipulovat se zařízením a ostatními komponenty.

Jde zde především o to zajistit datové média apod. k dalšímu odbornému zkoumání ve forenzních laboratořích. I bez dostupné techniky zaznamenáváme **tyto operace:**

- počet a typ stolních počítačů
- počet a typ jiných výpočetních zařízení
- analyzujeme jejich přístup do sítě
- vyslechneme příslušný personál, který má přístup do systému či na místo činu (administrátoři, správce sítě, aj.)
- identifikovat a zaznamenat počet disků, médií včetně přenosných zařízení
- identifikovat použité OS
- zhodnotit stav celého místa
- určit místa vhodné ke skladování (mimo místo činu)
- vytvořit si telefonní seznam na vnější dostupné zdroje (dodavatelé technického nebo SW vybavení, servisní firma

Obrázek 20 materiální a digitální místo činu [13]

Nejprve musíme vyhodnotit situaci a rozhodnout, kde se bude zkoumání důkazních materiálů provádět. Obvykle analýza dat probíhá v kontrolovatelném specializovaném laboratorním prostředí. U velkých komerčních firem se může stát, že situace vyžaduje

neprodlené a neodkladné vyšetření na místě činu, nebo se zde nachází rozsáhlé počítačové systémy využívající nejmodernější dostupnou technologii, která vyžaduje spolupráci s počítačovými experty (výrobci, správci systémů apod.). Tito odborníci zvolí nejlepší způsob zajištění zkoumaného objektu, popřípadě provedou kopie na záznamové médium.
Někdy se může stát, že k forenzní analýze **potřebujeme "živý"(zapnutý) systém,** nebo jsou data centralizovaně ukládána mimo počítač, obvykle na **SAN** (storage area network – dedikovaná datová síť soužící pro připojení externích zařízení k serverům). Je jasné, že zde **musí probíhat forenzní analýza přímo na místě**, proto se na ní musíme co nejlépe připravit a zvážit další faktory jako je:

- **čas**, který potřebujeme k provedení takového zkoumání a dohledný čas k dokončení analýzy
- **personální obsazení:** zda-li je personál dostatečně zkušený, proškolený a dokáže si poradit s takovouto situací
- **vhodná výbava:** jestli máme všechno potřebné vybavení k analýze dat na místě činu
- **dopad na činnost podniku:** při zdlouhavém zkoumání může mít naše činnost negativní dopad na např. obchodní činnost podniku
- **logistické a personální zájmy** zúčastněných osob při dlouhodobém rozmístění

7.2.2 Domovní prohlídka, prohlídka ostatních bytových prostorů

Dle zákonného ustanovení § 89 odst. 1 trestního řádu se vykonává domovní prohlídka, za předpokladu, že v bytových nebo v ostatních prostorech, určených k bydlení, jenž k nim náleží, se vyskytuje osoba nebo věc nezbytná pro trestní řízení.

V okamžiku kdy dostaneme povolení k domovní prohlídce, zajišťujeme výpočetní techniku (záznamová paměťová média, PC, DVD disky, harddisky, aj.) pro forenzní analýzu digitálních dat a další věci mající logickou a věcnou souvislost s vyšetřovanou událostí (zápisníky, poznámky, telefonní seznamy, apod.).

Vyšetřující orgán, který prohlídku provádí je povinen umožnit majiteli, či osobě v podnájmu, přítomnost během domovní prohlídky, **nezbytná je i účast nezainteresované třetí strany.**

7.2.3 Vnější prohlídka stop

U zajištěného důkazního materiálu nejprve provádíme tzv. vnější prohlídku, jde tedy o dokumentaci předmětů v době dodání ještě před jejich zkoumáním, kterou obvykle provádíme s spolu: s:

- posouzením a fotodokumentací balení a neporušenosti pečetí, či jejich nedostatky a možné příčiny porušení,
- posouzením a fotodokumentací samotných zařízení, jejich vnějších porušení, chybějících či nefunkčních částí spolu s výrobními kódy, sériovými čísly aj.,
- fotodokumentací vnitřních komponentů (paměťové disky, rozšiřující karty sloty, mechaniky) spolu s jejich vzájemným zapojením, které se provádí po odstranění casu (skříně počítače),
- detailnější prohlídkou určitých komponentů, ke kterým se váže povaha trestného činu, nejčastěji se jedná o paměťové disky, které chceme dokumentovat. Musíme je tedy nejprve odpojit a vyjmout, abychom měli přístup ke všem potřebným informacím o disku (značka, velikost, nastavení jumperů, interface disku apod.) a o jeho stavu (poškození ochranných pečetí, elektroniky aj.).

7.2.3.1 Skladování počítačových důkazů

Aby nedošlo k manipulaci se zajištěným zařízením, musíme ho prokazatelně a spolehlivě zabezpečit. Všechna zajištěná zařízení umísťujeme buď do původních, nebo do předem připravených obalů, které jsou příslušně a průkazně označeny, kvůli možné záměně. Obal je neprodyšně uzavřen a zabraňuje tak poškození či neoprávněné manipulaci s daty, alespoň do doby, než na nich začne pracovat příslušný specialista.

Musíme si dát velký pozor na způsob balení, aby nedošlo ke ztrátě dat, proto se musíme vyvarovat balit datová zařízení do obalů umožňující průnik elektromagnetického pole, či jiného záření (např. magnetická zařízení vymaže elektromagnetické pole).

7.3 Získání dat

Jelikož jsou digitální data“ materiál“, který můžeme lehce poškodit, či pozměnit, ať již úmyslně nebo neúmyslně, musíme zajistit v průběhu jejich zkoumání dokonalou integritu.

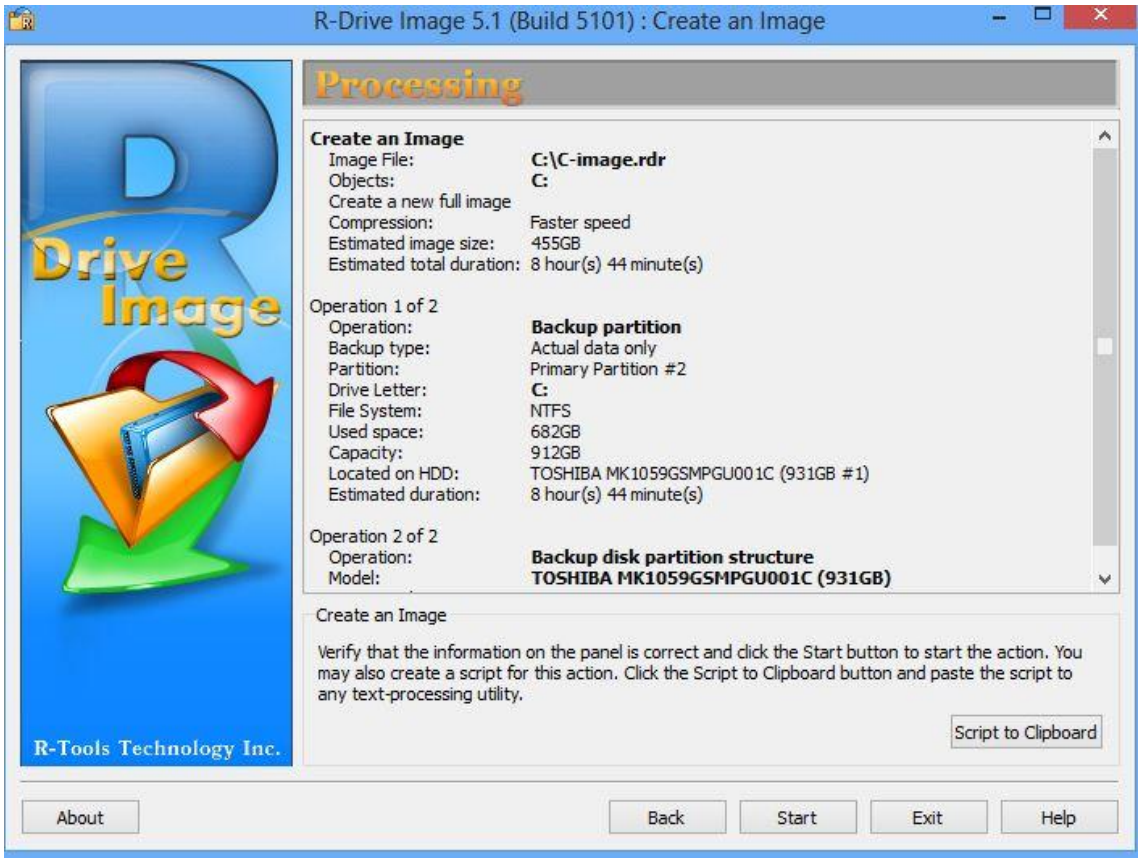
V opačném případě se taková data stávají nevhodná, protože zkoumání upravených dat by mohlo být zavádějící a nepřesné.

7.3.1 Záloha dat pomocí forenzní duplikace

Jak už bylo nastíněno v kapitole 4**, vytvoříme kopii, nebo duplikát digitálních dat**, aby nebyl původní důkazní materiál nějak modifikován, či porušen a tak ztratil svou věrohodnost.

Z pohledu HW můžeme k vytvoření duplikace použít **3 různé způsoby**. Asi nejuniverzálnější metoda je, že zkoumaný disk určený k duplikaci odpojíme a **připojíme ho k rozhraní našeho zařízení.**

Další možností je, že **ke zkoumanému PC připojíme další disk**, na který posléze vytvoříme obraz zkoumaného disku.



Obrázek 21 příklad vytvoření obrazu disku pomocí aplikace R-Drive

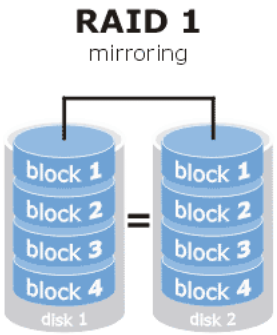
Poslední možností je, že zkoumaný **disk zkopírujeme přes síť.** Tuto síť musíme uzavřít, abychom eliminovali průnik třetí osoby a následnou manipulaci s daty. K lepší bezpečnosti používáme hashování. V tomto kroku se musíme vyvarovat hashovacích funkcí ve kterých byla kolize (MD4,SHA-0, aj.).

Nikdy tuto duplikaci neprovádíme pomocí zkoumaného systému! Jestliže připojíme disk, na který budeme kopírovat obraz disku nebo budeme vytvářet obraz přes síť, je

potřeba nabootovat OS z nějakého datového média (flash disk, DVD, aj.). K tomuto nám slouží speciální "live" OS vytvořené právě k těmto účelům, nebo systémy na bázi Unixu.

Programy vytvářející obraz disku musí umět zkopírovat všechna data od počáteční stopy až po služební stopu. Může se také stát, že některý cluster (sektor) disku nelze přečíst a proto je potřeba dané místo zaplnit clusterem stejné délky předem určeným obsahem. Tyto programy musí také zajišťovat další funkce např. kontrolu integrity (tzn., že by měl mít obraz stejné parametry jako zkoumaný disk, více kap. 5), proto je vhodné si tyto informace zjistit z nějakého bechmarku (testovací SW), nebo z Biosu (firmware pro osobní PC).

Toto zrcadlení je možné nastavit automaticky během normálního užívání PC např. pomocí diskového pole RAID 1.



Obrázek 22 zrcadlení pomocí diskového pole RAID 1

7.3.1.1 Vytvoření zálohy dat pomocí znalce

Dle zákonného ustanovení § 105 odst. 1 trestního řádu rozhoduje trestní orgán činný v trestním řízení o povolání znalce, vyžadují-li to okolnosti z plynoucí z vyšetřování v rámci trestního řízení. Tento postup samozřejmě neplatí pro interní šetření organizace, ale jen v případě, pokud jde o účely vyšetřování v rámci trestního řízení. Při soudním řízení rozhoduje o povolání znalce předseda senátu, který se ale v jednoduchých případech může spokojit "pouze" s vyjádřením příslušného státního orgánu nebo jiné právnické či fyzické osoby, kde nejsou pochybnosti o jeho správnosti.

Obrázek 23 soudní znalec

8 VYUŽÍTÍ FORENZNÍCH METOD K ODHALOVÁNÍ POČÍTAČOVÉ KRIMINALITY

O forenzních metodách používající se ve výpočetní technice můžeme říci, že jsou to speciální vědecké nástroje a postupy, které nám pomáhají odhalit pachatele při páchání trestné činnosti.

V následující kapitole si ukážeme praktické využití těchto forenzních metod.

8.1 Typické vyšetřovací situace

Při vyšetřování počítačové kriminality se setkáváme zejména s následujícími počátečními situacemi:

A. Zjištěné skutečnosti nasvědčují tomu, že se stal skutek, v němž je možno spatřovat trestný čin, nedovolují však vyslovit jednoznačný závěr o totožnosti pachatele (pachatelů) a o způsobu spáchání trestného činu. Způsobená škoda (nebo jiný následek) je či není patřičně zjištěna, přičemž lze nebo nelze z dosud shromážděných materiálů usuzovat na motiv činu.

B. Zjištěné skutečnosti nasvědčují tomu, že se stal skutek v němž je spatřován trestný čin a objasňují způsob spáchání trestného činu. Nedovolují však vyslovit závěr o totožnosti pachatele. Způsobená škoda (nebo jiný následek) je či není patřičně zjištěna, přičemž ze shromážděných materiálů lze nebo nelze usuzovat na motiv činu.

C. Zjištěné skutečnosti nasvědčují tomu, že se stal skutek, v němž je spatřován trestný čin, dovolují učinit závěr o totožnosti pachatele, nedovolují však vyslovit jednoznačný závěr o způsobu spáchání trestného činu. Způsobená škoda (nebo jiný následek) je či není patřičně zjištěna, přičemž lze nebo nelze z dosud shromážděných materiálů usuzovat na motiv činu.

D. Zjištěné skutečnosti nasvědčují tomu, že se stal skutek v němž lze spatřovat trestný čin, dovolující učinit závěr o totožnosti pachatele (pachatelů) a objasňují i způsob páchání. Způsobená škoda nebo jiný následek je či není patřičně zjištěna, přičemž lze či nelze usuzovat na motiv činu. [1]

8.2 Vyšetřování typických situací

Pro demonstraci využití forenzních metod si pro případ zkusíme vyšetřit fiktivní příklad počítačové kriminality.

Dejme tomu, že vlastníme firmu, kde se ztrácejí důležité interní informace o vývoji technologií. K těmto informacím má přístup pouze majitel (tedy my) a jeden zaměstnanec, který vede vývojovou divizi naší organizace.

Z těchto skutečností plyne, že hlavní podezřelý je již zmiňovaný zaměstnanec, protože není příliš pravděpodobné, že se k těmto informacím mohl dostat někdo jiný.

Proto neprodleně podáme trestní oznámení na podezření tohoto zaměstnance ze spáchání trestného činu dle **§§ 230 a 231 TZ**.

Na náš podnět policie započne vyšetřování výslechem podávajícího trestní oznámení, dále obviněného, popřípadě další osob mající nějakou spojitost s vyšetřovaným deliktem. Započne úkon **ohledání místa činu**, kde zajistí všechny potřebné materiální i digitální stopy.

Jakmile policie identifikuje a zdokumentuje všechen důkazní materiál, probíhá nasazení **forenzních metod k další analýze a forenznímu zkoumání.**

V našem fiktivním případě budeme řešit **situaci C**.

8.2.1 Obecný postup vyšetřování typické situace (C)

Obecný postup při řešení této situace je, že kriminalista nejprve neprodleně provede všechny příslušné zajišťovací úkony za účelem zajištění místa činu kvůli expertnímu zkoumání, především v oblasti IT a účetnictví a poté **v průběhu trestního řízení** (vyšetřování) **sdělí podezřelému obvinění**. Spolu s příslušnými specialisty si vytyčí všechny kriminalistické verze k objasnění, jakým způsobem byl trestný čin proveden.

Další nezbytný krok je **vyslechnutí obviněného**, všech případných svědků a ostatních znalců či specialistů. Zaměříme se zde především na objasnění a dokázání způsobu spáchání takového činu.

Pokud **obviněný spolupracuje** a sdělí nám technické detaily způsobu provedení, motiv apod., je vhodné vše sepsat do protokolu, který bude předložen příslušným znalcům pro lepší orientaci při znaleckém zkoumání, popřípadě pro **potvrzení či vyvrácení** takového tvrzení.

Může se stát, že obviněný využije svého zákonného **práva nevypovídat**, proto musíme naše úsilí zaměřit k zajištění jiných potřebných důkazů potřebných k dokázání způsobu páchání. Tyto důkazy mohou být např. závěry z provedené expertízy či vyšetřovacího experimentu.

Kriminalista si musí uvědomovat, že vyšetřování přešlo ze své počáteční fáze do **etapy dokazování,** musíme tedy obstarat nezbytné důkazy, které prokáží nabytí skutkové podstaty trestného činu.

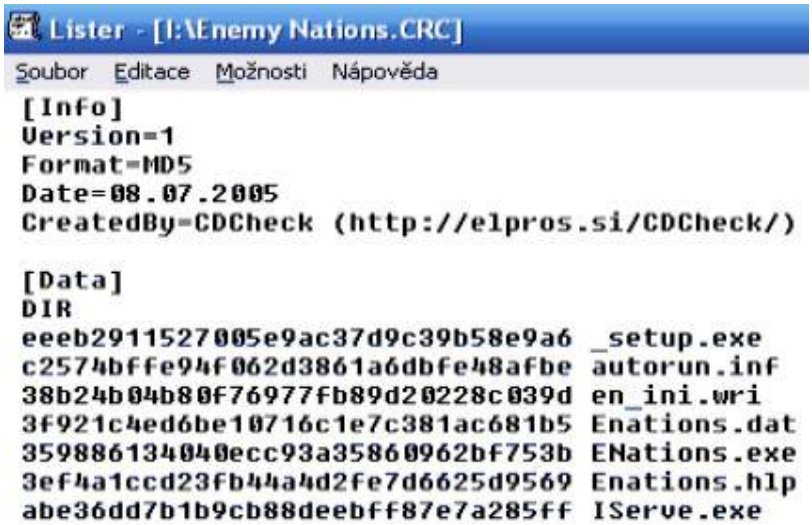
8.3 Praktický postup při forenzní analýze dat

Pro zkoumání dat z naší fiktivní situace **aplikuje policie metody forenzního zkoumání**. Prvním krokem bude zálohování dat soudním znalcem. Protože místo činu patří velké organizaci a je na něm nepřetržitý provoz, nemůžeme zkoumat digitální stopy přímo na pracovišti, a proto jej nebudeme zajišťovat. Zajištěný důkazní materiál podrobíme zkoumání ve speciálních forenzních laboratořích, ale ještě před začátkem analýzy provedeme zálohu těchto dat.

8.3.1 Autentizace a ochrana integrity

Pokud to situace dovoluje, měla by být zapnuta ochrana proti zápisu (vyměnitelné zařízení), či využito speciálních zařízení k ochraně proti zápisu (fyzické disky, aj.), kvůli zachování integrity.

Znalec obvykle provádí autentizace před pořízením kopie i po ní většinou pomocí hashování, aby bylo jisté, že soubory někdo nemodifikoval.



Obrázek 24 příklad hashovaného souboru

8.3.2 Postup zálohy dat

Nejprve odpojíme paměťové nosiče a napájení včetně datového kabelu od disku, či přímo ze základní desky, abychom disk nějak nepoškodili a aby data nikdo nemohl modifikovat.

Nyní musíme získat informace o konfiguraci systému pomocí kontrolovaného bootu.

K zachycení informací z BIOSu a kontroly jeho funkčnosti provedeme kontrolovaný boot. Je nezbytné zaznamenat:

1) ***boot sekvenci*** *– musíme se ujistit, že je nastaven požadovaný druh bootování např. z DVD disku, abychom byli schopni nabootovat. (pozn. tím můžeme pozměnit nastavení počítače)*
2) ***datum a čas*** *nastavený v BIOSu (může být záměrně rozdílný od skutečného)*
3) ***hesla a další potřebné informace*** *nezbytné pro vyšetřování případu*

K ověření schopnosti bootovat kontrolovaný systém z forenzního disku může být někdy nutné provést druhý kontrolovaný boot. Dále postupujeme:

1) *musíme ověřit, že* ***datový kabel i napájení jsou správně připojeny*** *k diskové mechanice a kabely z paměťových nosičů jsou naopak odpojeny*
2) *vložíme forenzní disk (zabrání náhodnému bootování z paměťových zařízení) do mechaniky a* ***nabootujeme****, přitom ověřujeme, že bootujeme právě z forenzního disku*
3) *jakmile je forenzní systém zaveden, provedeme specifické testy (mimo testování odpojených datových nosičů) k ověření funkčnosti a konfigurace*

Někdy si situace vyžaduje **testovat originální konfiguraci a nastavení disků** v originálním systému. K tomu potřebujeme:

1) *připojit disk k počítači a provést třetí kontrolovaný boot systému k získání informací o konfiguraci diskových nosičů* ***CMOS/BIOS***
2) *opět ověříme, že v mechanice máme forenzní boot disk*
3) *zjišťujeme především informace o konfiguraci diskových nosičů, zahrnující velikost disku* ***LBA*** *(logical block addresing),* ***počet cylindrů***, ***CHS*** *(hlavičku a sektory****), autodetekci*** *apod.*
4) *nyní vypneme počítač a disky odpojíme*

K získávání důkazů používáme výhradně systém znalce, musíme vždy dbát na to, aby znalecký systém disky zaručeně poznal.

Kopírování originálních dat provádíme vždy pomocí speciálních nástrojů, či programů pro ochranu zápisu.

8.3.3 Postup zálohy dat s využitím zkoumaného systému

V praxi jde pouze o výjimečný případ. Tento postup aplikujeme pouze v případě, když potřebujeme "živý systém" z důvodu:

- potřebujeme ověřit, zda-li byl počítač připojen k internetu (dočasná paměť)
- pole RAID neumožňuje individuální odpojení a získání dat, odpojení disku může znehodnotit tato data
- laptopové systémy nemusí umožňovat odpojení od systému, data takto můžeme znehodnotit, nebo je manipulace s diskem jen těžce přístupná
- nemáme k požadovaným úkonům všechno potřebné vybavení
- data jsou centralizovaně (většinou SAN) ukládána na server a proto je nutné využít síť

1) *opět připojíme nosiče (pokud jsme je odpojili) a ještě připojíme paměťové zařízení pro ukládání důkazního materiálu*
2) *nejprve se musíme navíc přesvědčit, že paměťové médium k ukládání stop je forenzně čisté*
3) *rozhodneme, jestli využijeme HW nebo SW ochranu zápisu (hrozba útoku přes síť) i během kopírování dat*
4) *poté nabootujeme forenzní OS*
5) *musíme si být jisti, že disk jenž bootujeme, bude forenzním systémem správně detekován*
6) *zvýšenou pozornost věnujeme dokumentaci všech zkušeností, protože je zde velké riziko manipulace s originálními daty. Zadokumentujeme i nestandardní chování systému, protože takové chování by mohlo způsobit porušení dat a v případě narušení jejich integrity v procesu získávání dat by bylo možno zjistit a zhodnotit míru vlivu těchto změn.*

8.3.4 Použití ochrany proti zápisu

K zajištění integrity dat využíváme ochranu proti zápisu. Tuto ochranu docílíme využitím specializované ochrany. Rozeznáváme dva základní typy ochrany, **hardwarovou a softwarovou.**

8.3.4.1 Postup použití HW ochrany proti zápisu

1) *k znaleckému počítači připojíme originální datové nosiče pro ochranu proti zápisu*
2) *nabootujeme znalecký systém spolu s forenzním OS*

8.3.4.2 Postup použití SW ochrany proti zápisu

1) *zapojíme originální disk k znaleckému systému*
2) nabootujeme systém znalce spolu s forenzním OS
3) po zavedení OS aktivujeme SW ochranu proti zápisu

Nyní prozkoumáme **geometrii** paměťových disků, abychom ověřili všechno volné místo spolu s host-protected oblastmi (tzn. specifická data např. v oblasti particion table, fyzická geometrie disku aj.).

Také zjistíme elektronické číslo disku spolu s ostatními uživatelskými přístupnými host-specific daty.

Kopii důkazního materiálu provádíme na paměťové medium znalce za použití speciálního typu SW, např.:

- SW balíček pro forenzní analýzu
- samostaný duplikační balíček
- disk manager net (síťová verze)

Pro kopii můžeme samozřejmě použít i speciální HW duplikační zařízení. Úspěšnost provedené kopie se většinou provádí pomocí hashování, hashový otisk porovnáme s originálním a v případě že je stejný, tak byla naše činnost úspěšná.

Další možností porovnání kopie a originálu je procházení disku sektor po sektoru.

Obrázek 25 sada Ultrakit [14]

8.4 Extrakce dat

Extrahováním se rozumí obnovením dat z paměťových médií, které byly pořízeny ze zajištěných paměťových nosičů. Rozlišujeme dva typy extrakce dat, **fyzický a logický.**

8.4.1 Fyzická extrakce dat

U tohoto typu extrahujeme vybraná data z paměťového nosiče na fyzické úrovni **bez ohledu na souborový systém** (např. FAT 32, NTFS aj.). To nám umožňuje využít následující metody: extrahování souborů, hledání dle klíčových slov, získání partition tabulek, informace o nevyužitém prostoru aj.

Vyhledávání dle klíčových slov využijeme zejména k zisku dat, která nejsou spojena s operačním ani souborovým systémem.

Vše provádíme pomocí speciálních utilit, které nám mohou pomoci u obnovování a získávání dat a souborů, které již byl smazány.

Zkoumání struktury partition nám umožní identifikovat souborové systémy a my můžeme určit, zda-li máme k dispozici celou fyzickou kapacitu disku.

8.4.2 Logická extrakce dat

V tomto typu extrakce je **extrahování založeno na platném souborovém systému** a data, která zde hledáme, jsou např. platné soubory, smazané soubory, skryté soubory, nepoužitý prostor logického disku. Následující postup zahrnuje tyto kroky:

1) ***vyšetříme souborový systém*** *s cílem zjištění těchto charakteristik:*

- *adresářová struktura*

- *atributy a jména souborů*
- *datové a časové značky*
- *velikost souborů a jejich umístění v adresářové struktuře*

2) *redukujeme data eliminací známých souborů (např. porovnáním vypočtených hash hodnot souborů s katalogem známých hodnot)*
3) *podle jména, přípony, hlavičky a umístění souboru na disku extrahujeme konkrétní data týkající se případu*
4) *obnovíme smazané soubory*
5) *získáme chráněná hesla a kódované, či komprimované soubory*
6) *získáme file slacky (soubory obsahující potencionálně náhodně vybrané bajty z dat paměti počítače)*
7) *zjistíme informace o nevyužitém diskovém prostoru*

8.5 Forenzní analýza dat

Je to proces interpretace získaných extrahovaných dat k určení jejich důležitosti k řešení vyšetřovaného úkonu. Mezi typické příklady forenzních analýz digitálních dat patří např. časová analýza, analýza skrytých dat, aplikací a souborů. Musí se také dokázat vlastnictví či modifikace dat uživatelem, a proto se obvykle "nasazuje" analýza vlastnictví a přechovávání.

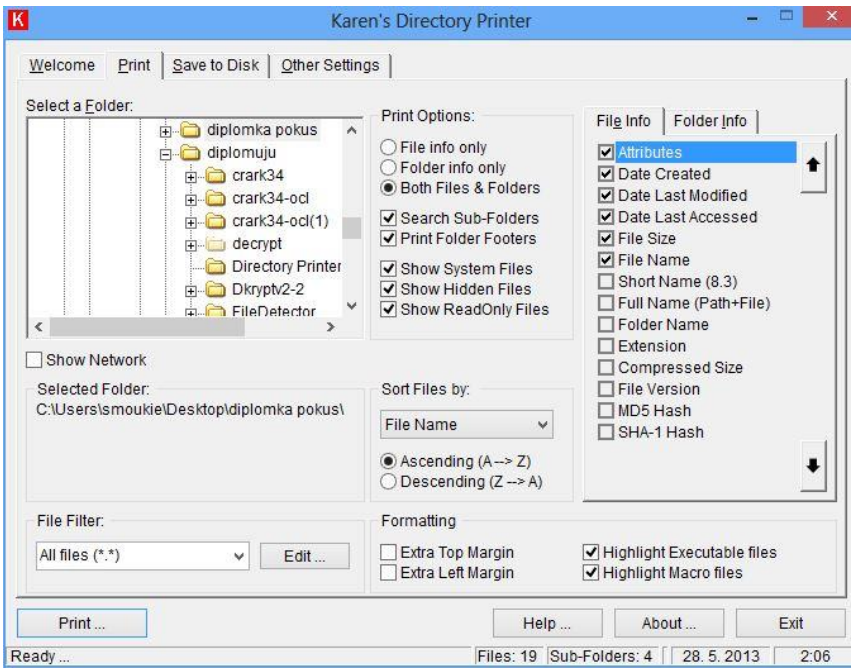
Tuto analýzu nejčastěji provádíme u:

a) **zkoumání pro účely trestního řízení**: soud vyžaduje, aby byl přítomen vyšetřování soudní znalec a kriminalistický expert
b) **zkoumání pro účely soudního řízení z jiných příčin než je podezření z trestného činu:** tuto analýzu provádí soudní znalec
c) **zkoumání na základě vyžádání fyzické nebo právnické osoby:** protože tato analýza probíhá mimosoudně, provádí ji povolaný expert (arbiter)

8.5.1 Druhy forenzních analýz digitálních dat

Ke konkrétnímu vyhledávání dat používáme dva druhy analýzy: **fyzický a logický**.

a) **fyzická analýza –** slouží k vyhledávání různých řetězců souborů, textových dokumentů, audio a video souborů apod., které jsou nezbytné k vyšetřování případu.



Obrázek 26 příklad vyhledávání dle řetězců pomocí aplikace Directory Printer

b) **logická analýza –** spočívá v analýze jednotlivých dat v "širším záběru" (detailněji), hledáme logické spojitosti s vyšetřovaným trestným činem.

8.5.2 Obecný postup forenzní analýzy

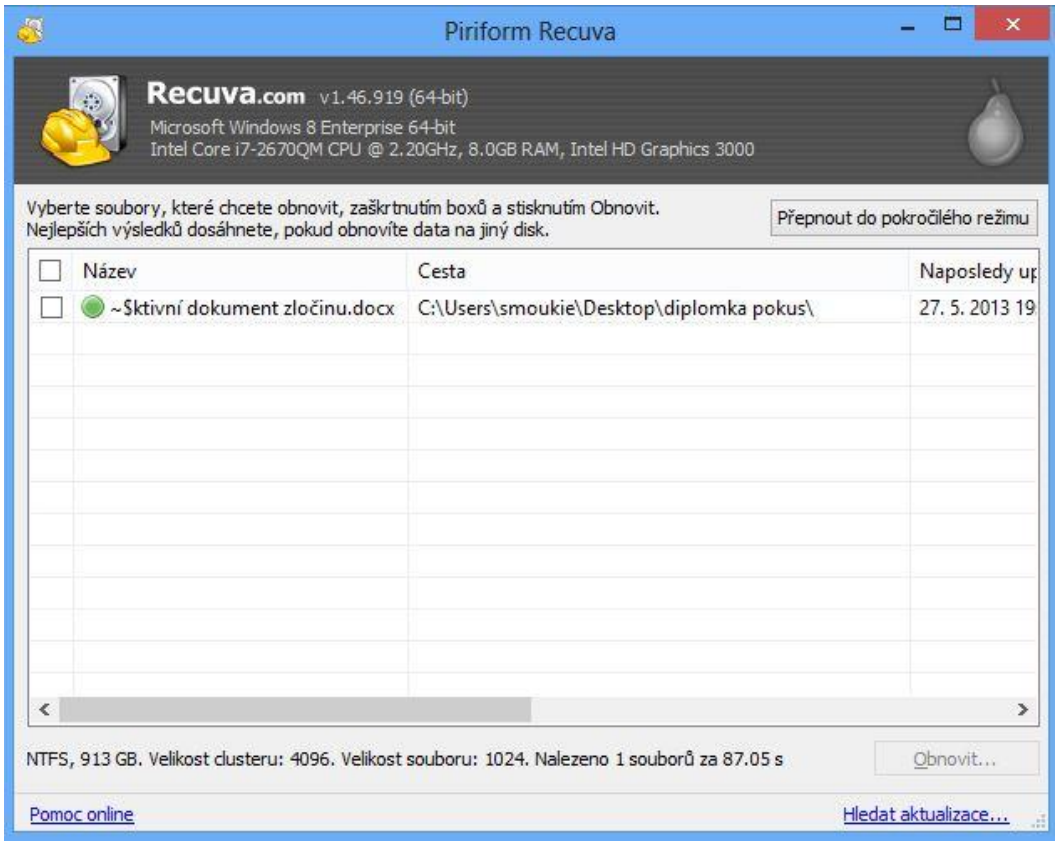
Při zkoumání počítače by nás měla zajímat **dočasná data** – tzn., že počítač by měl zůstat po detekci incidentu **ve fázi zapnuto!** Vypnutím počítače tato data (a tím pádem i potenciální důkazy) ztratíme. To ovšem představuje práci na „živém" systému, a my jakožto vyšetřovatelé můžeme některé potenciální důkazy nechtěně znehodnotit. Kromě toho, že bychom měli v této oblasti mít **dostatečné znalosti**, abychom nenapáchali velké škody, je potřeba také každý náš krok pečlivě **dokumentovat.**

Mezi dočasná data patří například obsah vyrovnávací a operační paměti, informace o síťových spojeních, informace o běžících procesech atd. Pokud tato data pro vyšetřování nepotřebujete (například nevyšetřujete případ, kdy je relevantním prvkem síť – útok skrze síť), raději takovou analýzu vůbec nedělámе. Jedná se o proces náročnější, než je analýza duplikovaného systému, a můžete si tím zbytečně zmařit další vyšetřování. [2]

Musíme vždy zajistit nedotknutelnost důkazního materiálu, aby nebylo se soubory již nijak manipulováno a zabránit tak jejich poškození, či ztrátě. V praxi se obvykle používá **forenzní duplikace** (tzn. záloha paměťových médií od první až po poslední stopu do obrazu disku, včetně smazaných souborů, odstraněných particion disku (odílů) aj.),

zkoumaného digitálního média. Zkoumání pak tedy probíhá na tomto obraze, ale jenom tehdy, když máme dostatek času pro vyšetřování a chceme zabránit např. přemazání přístupových časů.

Také může nastat situace, kdy byla již všechna data z paměťových medií smazána, či je paměťové médium nějak poškozeno, ale i přesto existuje způsob, jak tato data obnovit. Tato metoda se **nazývá forenzní záchrana dat.**



Obrázek 27 příklad forenzní záchrany dat pomocí aplikace Recuva

8.5.3 Praktický postup forenzní analýzy dat

Analýzou rozumíme interpretaci získaných extrahovaných dat a určení jejich důležitosti pro vyšetřování trestného činu. U této analýzy musíme vědět, že všechny časové údaje se odvíjí od nastavení v BIOSu, které je možné uživatelsky upravit.

8.5.3.1 Postup časové analýzy

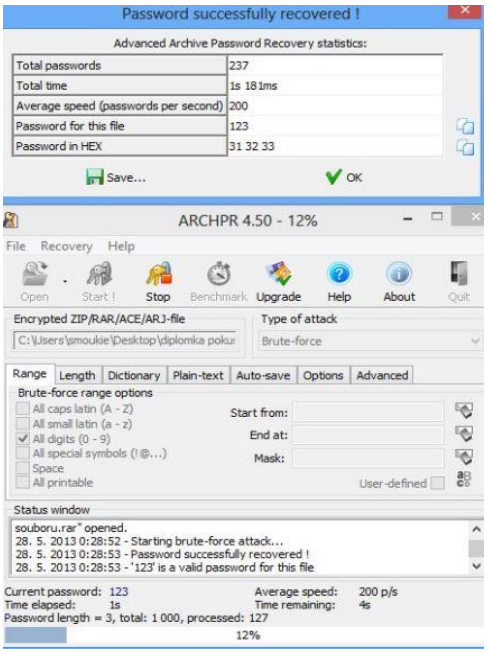
Pomocí časové analýzy můžeme určit posloupnost věcí, jenž se staly, nebo můžeme určit kdo a kdy na počítači pracoval. Obvykle využíváme dva typy postupu.

a) *V první řadě prozkoumáme datové a časové značky obsažené v adresářové či souborové struktuře, popřípadě metadatech (tzn. poslední modifikace, poslední přístup, čas vytvoření, tisku aj.) Díky těmto informacím logicky spojíme časovou posloupnost týkající se případu.*
b) *Prozkoumáním systémových logů o provozu aplikací, např. záznamy o chybách, instalacích, bezpečnostní záznamy aj. Např. když prozkoumáme bezpečnostní záznam, můžeme se dozvědět, který uživatel se kdy přihlásil na tuto pracovní stanici.*

8.5.3.2 Postup analýzy skrytých dat

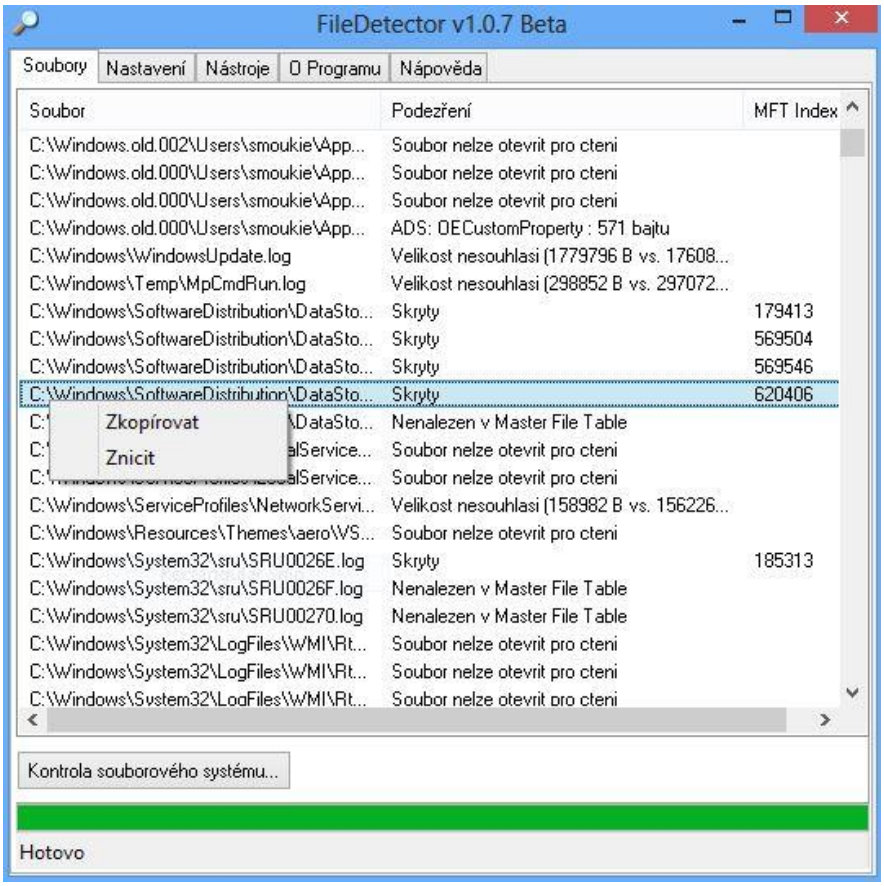
Některá data na disku bývají ať již úmyslně či neúmyslně skryta. Tato analýza slouží právě k odhalení a obnově takových dat a může objektivně vypovědět o znalostech výpočetní techniky podezřelého, pokud dokázal data vědomě skrýt. V praxi nejčastěji využíváme tyto metody:

1) *v první řadě* ***zharmonizujeme hlavičky a přípony*** *souborů, rozpoznali jakýkoliv nesoulad*
2) *následuje získání přístupu ke všem* ***zakódovaným, zkomprimovaným a ostatním heslem chráněným souborům****, které by mohla nastínit pokus data skrýt před neoprávněnými uživateli, k tomu je ale nezbytné zjistit heslo, jenž je stejně důležité jako samotný obsah souboru*



Obrázek 28 příklad prolomení zaheslovaného archivu pomocí aplikace ARCHPR

3) *získáme přístup ke skrytým datům pomocí **steganografie** (disciplína snažící se utajit komunikaci prostřednictvím ukrytí zpráv)*
4) *prověříme **HPA** (host-protected) oblast, výskyt souborů zde může nastiňovat pokus o úmyslné skrytí dat*



Obrázek 29 příklad podezřelých dat pomocí aplikace FileDetector

8.5.3.3 Postup analýzy aplikací a souborů

Důležité informace pro vyšetřování mohou být obsaženy přímo v aplikacích nebo souborech a mohou nám pomoci objasnit vědomosti uživatele a potenciál systému. Výsledky této analýzy nás nasměrují k dalším krokům zkoumání v procesu získávání informací (digitální i fyzické), případně dalších analýz. Musíme podniknout tyto kroky:

1) *podle důležitosti přezkoumáme jména souborů a již dle programového vybavení a existence určitých souborů určíme potencionálně neobvyklý způsob práce s aplikacemi*
2) *prozkoumáme obsah souborů*
3) *detekujeme druhy a počty OS*

4) *zharmonizujeme soubory vůči nainstalovaným aplikacím na disku*
5) *určíme vztahy mezi soubory (např. vztahy mezi internetovou historií a souborů case, nebo e-mailovou poštou a příloh)*
6) *identifikujeme neznámý typ souborů a stanovíme jejich důležitost pro vyšetřování*
7) *přezkoumáme všechny typické místa ukládání soborů a aplikací na disku, zda-li byly ukládány standardně nebo na jiné místa disku*
8) *přezkoumáme uživatelské nastavení a konfigurace*
9) *zanalyzujeme všechny metadata (tzn. obsah, který vytvořil uživatel obsahující navíc informace, které se nezobrazí při běžné činnosti s aplikacemi, jimiž byl soubor vytvořen)*

Obrázek 30 příklad prolomení internetového hesla pomocí aplikace Password Breaker

8.5.3.4 Postup analýzy vlastnictví a přechovávání

V některých případech může být nejpodstatnější identifikovat jednoho nebo více jedinců, kteří vytvořili, modifikovali nebo se jiným způsobem dostali do styku se souborem. Může být také důležité určit vlastnictví a vědomé přechovávání dotyčných dat. Prvky vědomého přechovávání jsou založeny na analýzách popsaných výše, zahrnujících jeden nebo více z následujících faktorů:

- *umístění subjektu na počítači do určitého data a času může pomoci určit vlastnictví a přechovávání (časová analýza),*

- *žádané soubory se mohou nacházet v nestandardních lokacích (např. uživatelem vytvořený adresář s názvem „child porn“) – (analýza aplikací souborů),*
- *samotný název souboru může mít důkazní hodnotu a může napovídat na obsah souboru (analýza aplikací a souborů),*
- *skrytá data mohou naznačovat úmyslný pokus vyhnout se odhalení (analýza skrytých dat),*
- *jestliže se podaří obnovit hesla potřebná k přístupu k zakódovaným a heslem chráněným souborům, samotná hesla mohou indikovat vlastnictví a přechovávání (analýza skrytých dat),*
- *obsah souboru může naznačovat vlastnictví a přechovávání, pokud obsahuje informace pro uživatele specifické.*

```
COMMENT Computer: BALTAZAR
COMMENT User: smoukie
COMMENT Prepared: 01:16 28. 5. 2013
COMMENT Folder: C:\Users\smoukie\Desktop\diplomka pokus\
COMMENT Include Sub-Folders? Yes
COMMENT
FOLDER  C:\Users\smoukie\Desktop\diplomka pokus\        ------- 4       14      737 576 737 576
FILE    ---A----        28. 5. 2013 00:29       28. 5. 2013 00:29       28. 5. 2013 00:29       75 438  dešifrovaný soubor.JPG
FILE    -H-A----        27. 5. 2013 19:50       27. 5. 2013 19:50       27. 5. 2013 19:50       162     fiktivni.pokus.zlocinu.docx
FILE    ---A----        27. 5. 2013 21:47       27. 5. 2013 21:47       27. 5. 2013 21:47       162     koD_fiktivni.pokus.zlocinu.docx
FILE    ---A----        28. 5. 2013 00:18       28. 5. 2013 00:18       28. 5. 2013 00:18       199     koD_fiktivni.pokus.zlocinu.rar
FILE    ---A----        28. 5. 2013 00:57       28. 5. 2013 00:57       28. 5. 2013 00:57       86 698  modifikace.JPG
FILE    ---A----        27. 5. 2013 21:49       27. 5. 2013 21:49       27. 5. 2013 21:49       19 176  neotevřetelný šifrovaný dokument.JPG
FILE    ---A----        27. 5. 2013 19:54       27. 5. 2013 19:54       27. 5. 2013 19:54       60 670  obnovení souboru.JPG
FILE    ---A----        27. 5. 2013 22:27       27. 5. 2013 22:27       27. 5. 2013 22:27       99 378  podezřelé soubory 2.JPG
FILE    ---A----        27. 5. 2013 22:19       27. 5. 2013 22:19       27. 5. 2013 22:19       100 381 podezřelé soubory.JPG
FILE    ---A----        27. 5. 2013 22:54       27. 5. 2013 22:54       27. 5. 2013 22:54       28 502  prolomení raru.JPG
FILE    ---A----        28. 5. 2013 01:05       28. 5. 2013 01:05       28. 5. 2013 01:05       49 976  rozluštění internetového hesla.JPG
FILE    -HSA----        27. 5. 2013 20:10       28. 5. 2013 01:05       27. 5. 2013 20:10       125 440 Thumbs.db
FILE    ---A----        28. 5. 2013 00:18       28. 5. 2013 00:18       28. 5. 2013 00:18       56 122  zaheslování souboru.JPG
FILE    ---A----        28. 5. 2013 00:27       28. 5. 2013 00:27       28. 5. 2013 00:27       35 272  zaheslování souboru.rar
FOLDER  C:\Users\smoukie\Desktop\diplomka pokus\dešifr\ ------- 0       4       1 448 386       1 448 386
FILE    ---A---X        27. 5. 2013 21:52       18. 1. 2006 12:44       27. 5. 2013 21:52       1 444 056       codder.exe
FILE    ---A----        27. 5. 2013 21:52       27. 5. 2013 21:52       27. 5. 2013 21:52       72      codder.ini
FILE    ---A----        27. 5. 2013 21:52       27. 5. 2013 21:52       27. 5. 2013 21:52       4 096   diplomka.sif
FILE    ---A----        27. 5. 2013 21:53       27. 5. 2013 21:47       27. 5. 2013 21:53       162     koD_fiktivni.pokus.zlocinu.docx
TOTAL   C:\Users\smoukie\Desktop\diplomka pokus\dešifr\ ------- 0       4       1 448 386       1 448 386
FOLDER  C:\Users\smoukie\Desktop\diplomka pokus\fiktivni.dukaz.kriminality\     ------- 0       0       0       0
TOTAL   C:\Users\smoukie\Desktop\diplomka pokus\fiktivni.dukaz.kriminality\     ------- 0       0       0       0
FOLDER  C:\Users\smoukie\Desktop\diplomka pokus\koD_fiktivni.pokus.zlocinu\     ------- 0       1       162     162
FILE    ---A----        28. 5. 2013 00:23       27. 5. 2013 21:47       28. 5. 2013 00:23       162     koD_fiktivni.pokus.zlocinu.docx
TOTAL   C:\Users\smoukie\Desktop\diplomka pokus\koD_fiktivni.pokus.zlocinu\     ------- 0       1       162     162
FOLDER  C:\Users\smoukie\Desktop\diplomka pokus\koD_fiktivni.pokus.zlocinu2\    ------- 0       0       0       0
TOTAL   C:\Users\smoukie\Desktop\diplomka pokus\koD_fiktivni.pokus.zlocinu2\    ------- 0       0       0       0
TOTAL   C:\Users\smoukie\Desktop\diplomka pokus\        ------- 4       19      2 186 124       2 186 124
```

Obrázek 31 příklad analýzy souborů vlastnictví a modifikace pomocí aplikace Directory printer

Výsledky pořízené jakýmkoliv z těchto uvedených kroků nemusí být vždy dostatečné k vyvození závěru. Ale pokud se ně podíváme jako na celek, pak vztahy mezi jednotlivými výsledky mohou poskytnout komplexnější obrázek. Jako finální krok v procesu zkoumání se ujistíme, že výsledky získávání a analýzy důkazů zvažujeme v celé jejich šíři. K tomu je často nezbytné, aby se znalec seznámil s určitými detaily šetřeného případu, ze kterých je pak možné učinit komplexnější závěry znaleckého zkoumání.

Obecně platí, že čím více detailů o šetření jsou znalci známé, s tím vyšší pravděpodobností a přesností je možné nalézt relevantní informace a důkazy. [7]

8.6 Postup forenzní analýzy mobilního telefonu

V našem fiktivním případu jsme mimo digitálních nosičů dat zajistili ještě mobilní telefon a ten podrobili forenznímu zkoumání. Nyní si ukážeme praktické postupy ohledně forenzního zkoumání mobilního telefonu.

Jak tedy probíhá v praxi vyšetřování mobilního telefonu? Vyšetřovatel předá mobilní telefon znalci, který je vybaven potřebnými nástroji. Od tohoto okamžiku je nežádoucí, aby přístroj přijímal další zprávy nebo hovory.

1) *v první řadě předá vyšetřovatel mobilní telefon znalci k dalšímu zkoumání pomocí speciálních nástrojů,*
2) *nyní zajistímet telefon, aby nepřijímal SMS zprávy a hovory*
3) *v minulosti se využívalo odstínění (Faraday bag), ale toto řešení nebylo spolehlivé, v současnosti vyjmeme SIM kartu a pomocí speciálního SW, popřípadě HW nástroje provedeme její duplikát (zvolíme možnost duplikace s dopočítáváním (A38 Limit) – kvůli zablokování operátora)*

Výhodou takové SIM karty je, že se neidentifikuje do sítě operátora a zároveň telefon nerozezná, že to není původní SIM karta a nezačne automaticky mazat data, což se ve výjimečných případech může stát.

Další výhodou je, že nemusíme znát PIN (identifikační kód), který nám sice může sdělit operátor, ale to vyžaduje soudní příkaz a ne vždy máme čas ho obstarat.

4) *následuje připojení telefonu pomocí datového kabelu k počítači a spustíme SW pro forenzní analýzu mobilních telefonů, který zobrazí všechna data, která jsou uložena v telefonu a na paměťové kartě (při větším počtu karet je rychlejší analyzovat data pomocí čtečky zvlášť)*
5) *požadovaná data načteme na logické (srozumitelná strukturovaná prezentace dat), či fyzické úrovni (výpis obsahu interní paměti (memory dump) obsahující i data, která byla již smazána (výsledek je nejistý).*
6) *data dále analyzujeme pomocí speciálních nástrojů např. Tovek Tools*
7) *zobrazíme zjištěná data (např. ve 3D síti s propojením vazeb)*

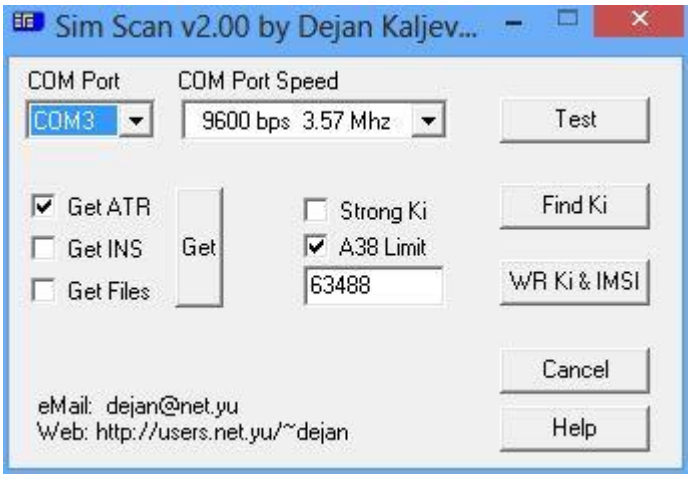
Největší komplikace těchto nástrojů je kompatibilita telefonů s nástroji, běžně se stává, že na evropské telefony nefungují americké nástroje nebo poskytnou méně dat, než potřebujeme k vyšetřování a naopak. Proto obvykle vyšetřovatel vlastní více takových nástrojů.

Tyto nástroje slouží jen jako doplňující údaje k případu a jejich důležitost posoudí až soud.

8.6.1 Tvorba duplikace SIM karty

Na výrobu duplikace SIM karty budeme potřebovat vhodný SW a čtečku karet. Pro příklad jsme použili program SIM_SCAN 2.00. Postup je tedy následující:

1) *spustíme program SIM_SCAN 2.00*
2) *zvolíme požadovaný port na který je připojena čtečka karet*



Obrázek 32 ukázka duplikace SIM karty pomocí aplikace SIM_ SCAN

3)zvolíme frekvenci 3.57 MHZ (standartní čtečka má 9600 bps)

4)zvolíme A38 Limit (pomalejší duplikace s dopočítáváním především u T-mobile)

5)spustíme vyčítání tlačítkem Find Ki

6)program nyní ověří přítomnost SIMky a komunikace s ní, pokud je vše v pořádku, začíná s vyčítáním

7)nyní nesmíme manipulovat s čtečkou nebo s kartou SIM

8)v adresáři SIM_SCAN v cílovém umístění programu nalezneme vypočtené KI a IMSI

9)zjištěné kódy nyní můžeme vložit do naprogramované karty a nová SIM karta je připravena k použití

8.7 Dokumentace

Dokumentací rozumíme **písemný detailní záznam o postupu naší činnosti** ve všech bodech. Hlavní zásady jsou především přehlednost, srozumitelnost, komplexnost a úplnost.

Velký pozor si dáváme na to, komu budeme tuto dokumentaci prezentovat a že jeho znalost v oblasti výpočetní techniky nemusí být na takové úrovni, aby vše správně pochopil, Proto se snažíme vystihnout všechno důležité srozumitelnou formou a do příloh přikládáme praktické výpisy z relací apod.

8.7.1 Postup znaleckého posudku

Dokumentaci se snažíme vždy vytvářet během forenzního zkoumání a měla by být v souladu s politikou forenzních laboratoří. Obecně se dá říci, že jsou to návrhy a vnitřní pravidla laboratoří vyžadující specifická psaní zprávy, např: logická posloupnost. Nezbytné náležitosti této zprávy jsou:

1) *identifikace laboratoře, která výzkum provedla*
2) *podací číslo případu nebo jiná identifikace*
3) *datum, kdy bylo zkoumání započato*
4) *datum ukončení zprávy*
5) *případně identita překladatele*
6) *seznam položek určených ke zkoumání, včetně jejich sériových čísel a typů*
7) *seznam všech požadavků, které nám byly zadány ke zkoumání*
8) *identita znalce*
9) *popis všech provedených kroků – např. hledání textových soborů aj.*
10) *celkové shrnutí provedené analýzy (např. odpovědi na zadané otázky)*

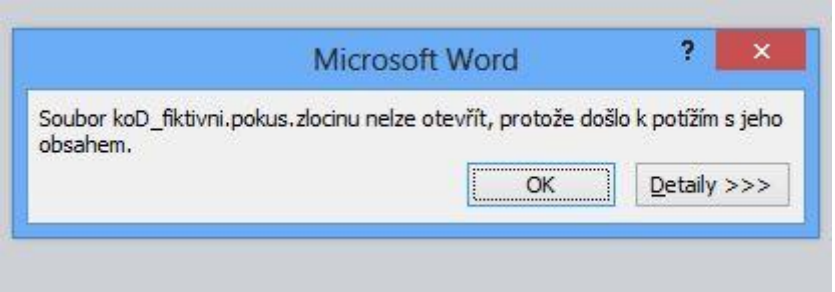
Všechna provedená shrnutí by měla být odvoditelná ze zprávy, kterou nám znalec předal.

8.7.1.1 Detaily nálezu

Detaily nálezu se rozumí:

1) specifické soubory, které po nás byly vyžadovány
2) ostatní podporující nálezy (včetně smazaných)
3) hledání dle klíčových slov nebo řetězců
4) výpis komunikací (chaty, diskusní fóra, icq, komunikace po síti aj.)

5) analýza grafických dat
6) důkazy o vlastnictví (datum registrací, či vytvoření dokumentů aj.)
7) analyzovaná data
8) popis všech využitých programů pro zkoumání položek
9) všechny techniky maskování (skryté atributy), či kryptografické metody (steganografie, šifrování)



Obrázek 33 příklad zaheslovaného souboru

K takovýmto výstupům je vhodné přidat navíc podporující materiály, kde jsou tiskové výstupy důkazů, digitální kopie důkazů, dokumentace zachování inegrity, výpisy z chatů aj.

Pro lepší orientaci se někdy využívá tzv. **Glosář**, což je odborný slovník technických výrazů sloužící k lepšímu pochopení dané problematiky.

ZÁVĚR

Závěrem chci říci, že tato problematika je ve skutečnosti mnohem složitější a má mnohem více aspektů a hledisek dělení. Nastínil jsem pouze základní rozdělení a způsoby forenzních postupů.

Během vypracovávání mé diplomové práce mne toto téma natolik zaujalo, že bych se chětl v budoucnosti forenzními metodami dále zabývat a podílet se na jejich zdokonalování, např. i ve svém budoucím zaměstnání.

Přínosem pro lepší dopadení a postižení nelegálních škodlivých narušitelů virtuálního světa je nově zpracovaná legislativa v čele s novelizovaným trestním zákoníkem č. 40/2009 Sb., popisující všechny trestné činy spojené s počítačovou kriminalitou.

Tato práce by mohla mít praktické využití jako metodický postup pro vyšetřovatele, ale především varovat.

Doporučil bych ji k přečtení i běžným uživatelům internetu, aby se mohli seznámit se zákeřným nebezpečím v kyberprostoru, které některé z nich může nevědomky nebo z neznalosti věci ohrozit. Zároveň je i varovat k opatrnosti v užívání mobilních a sociálních sítí, kde mohou jejich nevinné údaje zneužít útočníci ke své kriminální činnosti.

Každý uživatel by se měl chránit hlavně sám před sebou a “klikat“ pouze na známé a důvěryhodné odkazy. Svůj počítač by měl zabezpečit vhodným antivirovým programem, protože ochrana našich dat je dnes velmi důležitá a může mít klíčovou roli na obranu proti nelegálnímu, nemorálnímu a neoprávněnému zneužití údajů získaných prostřednictvím výpočetní techniky.

ZÁVĚR V ANGLIČTINĚ

To conclude it, i would like to say that those issues are even more difficuilt and have a lot of aspects and different points of view. I sketched only basic sorting and types of forensic methods.

During working on my diploma thesis I started to be really interested in this topic, so I would like to deal with the internet forencics more in the future and be part of its improvement, e.g. in my future job. Brand new legislations including the criminal Code nr. 40/2009 Sb. brings the improvement for better catching illegal users in cyber space and describes all kinds of cyber crime.

This thesis is supposed to warn, but it also might be used as a useful handbook for investigators.

I would recommend to read it also to ordinary internet users to get to know the treacherous danger from cyber space. Also to make them more careful, because it can put their data in danger without they even know it. It is important to deal really carefully with social and mobile networks, where their innocent data could be used by the offenders to commit the cyber crime. .

Every user should first of all take care of themselves and visit only known and trustworthy pages. The computers should be protected by a suitable anti-virus software, because it is important to protect our data and fight with illegal, immoral and unauthorized abuse, gained with using information technologies.

SEZNAM POUŽITÉ LITERATURY

[1] STRAUS, Jiří. Kriminalistická metodika. Plzeň : Aleš Čeněk s.r.o., 2006.

ISBN 80-86898-66-0. s. 271-286.

[2] KADLEC, Josef. Forenzní analýza digitálních dat. Hradec Králové, 2004. Dostupné z: http://i.iinfo.cz/files/root/k/Digitalni_forensni_analyza.pdf. Semestrální práce. Univerzita Hradec Králové. Vedoucí práce Miroslav Feltl.

[3] RAK, Roman a Viktor PORADA. Digitální stopy v kriminalistice a forenzních vědách. [online]. 2006, 1 - 21 [cit. 2013-05-28]. Dostupné z: www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf

[4]] ŠAMŠA, Václav. Metody záchrany dat při forenzním aud. Metody záchrany dat při forenzním aud [online]. [cit. 2013-05-28]. DOI: 224999777. Dostupné z: http://www.tdp-ontrack.cz/download/metody-zachrany-dat-pri-forenznim-auditu.pdf

[5] Smejkal, V. - Sokol, T. - Vlček, M.: Počítačové právo. Praha, C. H. Beck/SEVT 1995

[6] OBR, Jiří. Sniffing: Odposlech datové komunikace. Sniffing: Odposlech datové komunikace [online]. 2009 [cit. 2013-05-28]. Dostupné z: http://www.itbiz.cz/sniffing-odposlech-datove-komunikace

[7] KADLEC, Josef. Forenzní analýza. Forenzní analýza [online]. 2005 [cit. 2013-05-28]. Dostupné z: http://www.root.cz/clanky/forenzni-analyza

[8] Matějka, M.: Počítačová kriminalita. Praha : Vydavatelství a nakladatelství Computer Press, 2002, s. 18, [cit. 2013-05-28].

[9] ZÁKONY ON-LINE [online]. [cit. 2013-05-28]. Dostupné z <http://zakony-online.cz>.

[10] Počítačové sítě. Počítačové sítě [online]. [cit. 2013-05-28]. Dostupné z: http://www.arit.cz/sprava-siti.html

[11] STRAUS, Jiří. *Kriminalistická metodika*. Plzeň : Aleš Čeněk s.r.o., 2006.

ISBN 80-86898-66-0. s. 271-286 [cit. 2013-05-28].

[12] JIROVSKÝ, Václav. HNÍK, Václav. KRULÍK, Oldřich. *Základní definice, vztahující se k tématu kybernetických hrozeb.* [online]. 2006. [cit. 2013-05-28].

Dostupný z WWW: <http://www.mvcr.cz/bezpecnost/informacni/zakladni_info.pdf>.

[13] POŽÁR, Josef. *Možnosti odhalování informační kriminality a kyberterorismu* [online]. Praha : 2007 [cit. 2013-05-28]. Dostupný z WWW: <http://www.comguard.cz/fileadmin/user_upload/sbornik/01_Moznosti_odhalovani_informacni_kriminality_a_kyberterorismu.pdf>.

[14] *Forenzní zkoumání digitálních důkazů-příručka vyšetřovatele* [online]. 2005 [cit. 2013-05-28].Dostupný z WWW: http://www.rac.cz/rac/homepage.nsf/CZ/883AABB42333CB35C12570FC0034A328/$FILE/Guide%20051230.pdf>.

[15] DCIT. Prověření bezpečnosti mobilních aplikací. Prověření bezpečnosti mobilních aplikací [online]. 2013 [cit. 2013-05-28]. Dostupné z: http://www.dcit.cz/cs/bezpecnost/audit-mobilnich-aplikaci

[16] Počítačové viry. Počítačové viry [online]. 2009 [cit. 2013-05-28]. Dostupné z: http://www.web4men.eu/pg/pocitace/pocitacove-viry/?IdDir=822&Lang=1

[17] SHEPHERD, Carl. What is Phishing? And Why It's Important to You... What is Phishing? And Why It's Important to You... [online]. 2011 [cit. 2013-05-28]. Dostupné z: http://community.homeaway.com/blogs/homeaway-insights/2011/10/10/what-is-phishing-and-why-its-important-to-you

[18] PAXEL. Počítačová kriminalita a finanční krize. Počítačová kriminalita a finanční krize [online]. [cit. 2013-05-28]. Dostupné z: http://linkuj.cz/?id=show&viewnr=4&typ=0&par=65554

[19] ŠEBESTOVÁ, Marie. Popelkou informační bezpečnosti jsou spisovny a archivy. Popelkou informační bezpečnosti jsou spisovny a archivy [online]. 2011 [cit. 2013-05-28]. Dostupné z: http://www.cqs.cz/Novinky/Popelkou-informacni-bezpecnosti-jsou-spisovny-a-archivy.html

[20] VLAŠÍN, Mojmír. Proměny pojetí autorství a jeho paradoxy. Autorské právo a bezpráví reklamy [online]. 2011 [cit. 2013-05-28]. Dostupné z: http://www.kulturni-noviny.cz/nezavisle-vydavatelske-a-medialni-druzstvo/archiv/2013/5-2013/autorske-pravo

[21] KOPECKÝ, Kamil a Veronika KREJČÍ. RIZIKA VIRTUÁLNÍ KOMUNIKACE [online]. 2010 [cit. 2013-05-29]. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=10:brozura

[22] NYE, Joseph. Project Syndicate. Jestliže vznikne kyberválka, tak bude zatraceně i fyzicky bolet [online]. 2012 [cit. 2013-05-29]. Dostupné z: http://zpravy.idnes.cz/jestli-vznikne-kybervalka-tak-bude-zatracene-i-fyzicky-bolet-p5w-/kavarna.aspx?c=A120411_125541_kavarna_chu

[23] JANSONOVA, Petra. Kam se hrabou drogové kartely na kyberzločin. [online]. 2012 [cit. 2013-05-29]. Dostupné z: http://21stoleti.cz/blog/2012/02/29/kam-se-hrabou-drogove-kartely-na-kyberzlocin

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

OS Operační systém

FAT File Allocation Table – souborový systém

IP Internetový protokol

SW Software – programové vybavení

HW Hardware – fyzické vybavení

NTFS New technology file systém – souborový systém

IT Information technology – výpočetní technika

ICT Information and Communication Technologies – informační a komunikační technika

BIOS Basic Input-Output Systém – firmware pro osobní pc

CMOS Complementary Metal–Oxide–Semiconductor – využíván u integrovaných obvodů

SAN Storage area network – datová serverová sít

LAN Local area network – lokální dedikovaná sít

WAN Wide area network – rozsáhlá počítačová sít – (např. internet)

RAID Redundant Array of Independent disk – diskové pole

PC Personal computer – osobní počítač

HPA Host protected – chráněná oblast disku

SIM Subscriber identity module – identifikační karta do mobilního telefonu

IDS Intrusion Detection Systém – nástroj k identifikaci průniku do sítě

LBA Logical block adresing – metoda adresování bloků na disku

DNS Domain Name Systém – server s doménou

TCP/IP Transmission Control Protocol/Internet Protocol – protokol sítové vrstvy

ČR Česká republika

SEZNAM OBRÁZKŮ