Slovenská technická univerzita v Bratislave
FAKULTA INFORMATIKY A INFORMAČNÝCH TECHNOLÓGIÍ
Študijný program: Počítačové systémy a siete

KH Team

Integračné prostredie na forenzné analýzy

Tímový projekt

vedúci tímového projektu projektu: Ing. Adrián Bagala
členovia tímu: Bc. Michal Novák,
Bc. Michal Mikula,
Bc. Miroslav Staňo,
Bc. Michal Makový,
Bc. Miroslav Makýš,
Bc. Ivan Mrva

máj, 2007

Obsah

1 Zadanie

Pre pedagogické účely vytvorte WEB stránku demonštrujúcu princípy a činnosť forenznej analýzy. Analyzujte a posúďte dostupné voľne šíriteľné nástroje na forenznu analýzu. Navrhnite a implementujte integračné prostredie pre nástroje forenznej analýzy s cieľom vytvorenia jednotného prostredia na analýzu a záznam výsledkov analýzy.

Odporúčaná literatúra: 1. GRANCE, T., CHEVALIER, S., KENT, K., DANG, H.: Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response. NIST Special Publication 800-86. August 2006. 2. BREZINSKY, D.: Guidelines for Evidence Collection and Archiving. RFC 3227, February 2002.

2 Úvod

Počítače, digitálne médiá a zariadenia v mnohých rôznych podobách zohrávajú hlavnú rolu v rapídnom náraste kriminálnych činov po celom svete. Týmto zariadeniam sa v dnešnej dobe prakticky nevyhneme a asi si ťažko predstavíme život bez ich asistencie – či už ide o vedeckú alebo komerčnú sféru, alebo len o domáci osobný počítač. Ich vysoká dostupnosť zapríčinila zaradenie týchto prístrojov medzi bežné súčasti nášho každodenného života (hoci si to niekedy ani neuvedomujeme). Dáta môžu byť uložené alebo prenášané štandardnými počítačovými systémami (napr. pracovné stanice, prenosné počítače, servery), sieťovými zariadeniami (napr. „firewally“, smerovače), počítačovými periférami (napr. tlačiarne), osobnými elektronickými asistentmi (PDA), CD, DVD médiami, prenosnými pevnými diskami, „flash“ pamäťami, atď. Na ukladanie dát môžu byť použité aj mnohé elektronické zariadenia, akými sú napr. mobilné telefóny, hracie konzoly, elektronické audio prehrávače, digitálne videorekordéry a pod. Toto všetko sú formy, ktoré tieto zariadenia dosahujú. Postupom času budú pôvodné zariadenia, postupy a zvyky celkom nahradené týmito digitálnymi formami.

A práve stúpajúca dostupnosť a bežnosť sú hlavnými dôvodmi, prečo sa tieto zariadenia stávajú terčom a nástrojom zločinu. V dnešnej dobe je teda potrebné chrániť väčšinu informačných systémov, či už sa jedná o informačné systémy firemné, štátne alebo súkromné, chceme aby boli všetky služby poskytované týmito systémami bezpečné, spĺňali požiadavky legislatívy a regulačných orgánov, ale hlavne aby boli dôveryhodné z hľadiska používateľov využívajúcich tento systém. Preto bolo nutné vytvoriť vedu (resp. metódy), ktorá by takéto prostredie počítačov, sietí a všeobecne digitálnych dát skúmala.

Vo všeobecnosti môžeme povedať, že táto rekonštrukcia prebieha podobne aj v prípadoch, kde je potrebné skúmať počítače a iné digitálne zariadenia či iba dáta. Týmto sa zaoberá **forenzná analýza digitálnych dát** alebo inak **počítačová forenzná analýza** (angl. “digital forensics” alebo “computer forensics”).

Samozrejme, že medzi oblasťou skutočnosti a oblasťou digitálneho prostredia sú isté rozdiely. Digitálne dáta sú napríklad veľmi náchylné ku zmene, t.j. sú veľmi nestále. Tomu potom musí byť prispôsobené nakladanie s takýmito dátami, či už ide o samotný zber, uchovávanie alebo transport. Takýto zber dôkazov môže byť časovo veľmi náročný a to

predovšetkým v závislosti na množstvo skúmaných dát. Avšak na druhú stranu rekonštrukcia udalosti spravidla nie je náročná na fyzický priestor, takže je možné takúto rekonštrukciu previesť napríklad priamo v súdnej sieni.

3 Návrh riešenia

3.1 Hrubý návrh riešenia

Na základe analýzy problematiky forenzných techník testovania a nástrojov v zimnom semestri a špecifikácie produktu sme sa dohodli na nasledovných faktoch nami vyvíjaného nástroja na forenznu analýzu:

Aplikácia bude spúšťaná prostredníctvom zavedenia operačného systému na báze Linux nahratom na dopredu pripravenom "live" CD v móde "autorun" (automatické spustenie) s ostatnými, k behu nástroja potrebnými aplikáciami a službami.

Obraz ("image") časti alebo celého disku sa bude vytvárať na externé USB zariadenie po spustení aplikácie alebo bude možné zvoliť už vytvorený obraz disku určený na ďalšiu analýzu.

Na forenzné analyzovanie obrazu disku si bude môcť užívateľ vybrať dopredu nadefinovanú rutinu vykonávajúcu určitý druh analýzy, alebo si sám interaktívne zostaviť reťaz z programov dostupných v kolekcii nástrojov „The Sleuth Kit".

Výsledky prebehnutých analyzujúcich rutín budú vypisované priamo v okne aplikácie, resp. ich bude možné uložiť do výstupného súboru / súborov.

3.2 Návrh systému

3.2.1 *Výber a vytvorenie „live" CD distribúcie operačného systému*

Slovom „live" sa označujú tie distribúcie operačného systému, ktoré môžete spustiť priamo z CD, resp. DVD. Teda stačí nastaviť v „BIOS-e" zavádzanie systému z CD-ROM, vložiť CD, resp. DVD do mechaniky a reštartovať počítač. Distribúcia sa spustí priamo z vloženého CD, resp. DVD. Nemusíte teda nič inštalovať a ani zložito konfigurovať.

V súčasnosti je k dispozícií niekoľko voľne dostupných „live" distribúcií operačného systému postavenom na báze operačného systému Linux.

Na vytvorenie tohto „live" CD bola zvolená distribúcia s názvom **Slax**, ktorá nám umožňuje jednoducho pridávať rôzne balíky programov potrebných k spusteniu výslednej aplikácie. Navyše Slax poskytuje štandardne grafické prostredie KDE, ktoré vyhovuje naším potrebám pre spustenie výslednej aplikácie. Hardvérové požiadavky sú taktiež pomerne prijateľné – budú uvedené v systémovej príručke.

Po modifikovaní pôvodnej verzie tejto distribúcie - pridaní všetkých balíkov potrebných k behu výslednej aplikácie a zmenou rôznych nastavení kvôli efektívnemu a rýchlemu načítaniu operačného systému do pamäte počítača bude vytvorený ISO súbor predstavujúci obraz CD disku takto upravenej distribúcie.

3.2.2 *Výber implementačného prostredia aplikácie*

Výsledný produkt sme sa rozhodli implementovať ako webovú aplikáciou s využitím skriptovacieho jazyka PHP. K tejto voľbe nás viedla najmä tá skutočnosť, že zobrazovanie výstupov jednotlivých analýz by mohlo byť v niektorých prípadoch pomerne rozsiahle, čo však pri webovej aplikácií nie je žiaden problém. Ďalšími výhodami webovej aplikácie oproti klasickej „okienkovej“ aplikácii sú napr. dobré možnosti formátovania daných výstupov a možnosť vytvorenia prehľadnej navigácie v aplikácii.

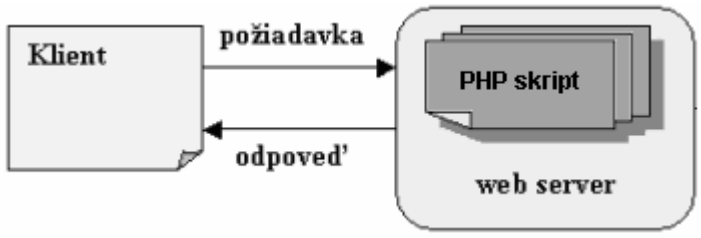
Hlavným kritériom pre výber skriptovacieho jazyka PHP boli najmä skúsenosti jednotlivých členov tímu s týmto jazykom.

3.2.3 *Základná architektúra aplikácie*

Z použitia skriptovacie jazyka PHP a tvorby dynamických webových stránok vyplýva, že výsledná aplikácia bude implementovaná ako klient/server architektúra, znázornená na nasledujúcom obrázku.

Pretože výsledná aplikácia bude spúšťaná z operačného systému zavádzaného z „live“ CD disku bude klient aj server vždy predstavovať jedna - tá istá pracovná stanica. Server (web server) je automaticky spustený po naštartovaní operačného systému ako tzv. „deamon“ proces (na pozadí). Klienta predstavuje v tomto prípade internetový prehliadač, ktorého okno s domovskou stránkou aplikácie bude taktiež spustené a zobrazené po naštartovaní operačného systému.

Detailnejší pohľad zobrazujúci princíp komunikácie medzi klientom a web serverom je znázornený na ďalšom obrázku.



Obr. 3.1 Princíp komunikácie medzi klientom a web serverom.

Klient prostredníctvom svojho internetového prehliadača vyšle na web server požiadavku, ktorá bude spracovaná jedným alebo viacerými PHP skriptami, ktoré po spracovaní požiadavky odošlú naspäť klientovi odpoveď. Táto odpoveď bude interpretovaná internetovým prehliadačom a následne zobrazená na obrazovku.

Podrobenejší opis tejto komunikácie a spôsob implementácie jednotlivých PHP skriptov bude bližšie opísaný v časti Implementácia.

3.2.4 *Návrh jednotlivých rutín forenznej analýzy*

Na analyzovanie obrazu súborového systému budú použité programy z kolekcie nástrojov „The Sleuth Kit“ určených na forenzné testovanie, ktoré sú akousi zbierkou voľne dostupných programov združených v jednom balíku s možnosťou ich spúšťania a zberaním výstupných údajov. V našej aplikácií sa budeme snažiť tieto programy združiť a integrovať do jedného nástroja poskytujúceho grafické rozhranie. Základnou koncepciou bude vytvorenie niekoľkých rutín ktoré budú pozostávať zo zreťazenia programov dostupných z kolekcie nástrojov „The Sleuth Kit“. Tieto rutiny (procedúry) budú potom zobrazovať informácie získané z výstupov jednotlivých programov pustených v rámci tejto rutiny v prehľadnom formáte. Taktiež bude existovať možnosť manuálneho spúšťania dostupných programov z kolekcie „The Sleuth Kit“ so zobrazením neformátovaného výstupu.

V nasledujúcom prehľade sú stručne opísané výstupy niektorých vybraných programov, ktoré sú súčasťou kolekcie „The Sleuth Kit“:

fsstat - zobrazuje detaily a štatistiky o súborovom systéme obrazu disku,

ffind - hľadá alokované a nealokované mená súborov, ktoré používajú daný „i-uzol“,

fls - vypíše zoznam alokovaných a zmazaných mien súborov v danom adresári („i-uzle“),

ils - vypíše zoznam informácií o jednotlivých „i-uzloch“,

ifind - nájde “meta-data” štruktúru, ktorá alokovala danú diskovú jednotku.

icat - vypíše súbor s daným číslom „i-uzla“ na štandardný výstup,

istat - zobrazí štatistiky a detaily o danom „i-uzle“,

dcat - zobrazí obsah dát danej dátovej jednotky (fragmentu) v ASCII alebo „hexa“ formáte,

dls - vypíše zoznam informácií o fragmentoch,

dstat - zobrazí status, či je daný fragment alokovaný,

mactime - vytvorí časovú líniu aktivít súborov,

sorter - triedi súbory uložené na obraze disku podľa typu.

V nasledujúcom prehľade sú špecifikované niektoré rutiny, ktoré máme v úmysle implementovať do integračného prostredia:

Systém súborov – bude poskytovať prehľad o súborovom systéme, bude umožňovať prehliadanie jednotlivých adresárov a bude poskytovať informácie o súboroch.

Vymazané súbory – bude poskytovať zoznam a informácie o vymazaných súborov na danom obraze.

Typy súborov – bude poskytovať prehľad o jednotlivých typoch súborov a zaradenie súborov do jednotlivých skupín.

Časové línie – bude poskytovať prehľad o aktivitách so súbormi v určitej časovej línii.

Meta dáta – bude poskytovať prehľad o alokovaných a nealokovaných „i-uzloch“ spolu s ďalšími špecifickými informáciami.

Dátové jednotky – bude poskytovať prehľad o dátových blokoch a bude vypisovať ich obsah v rôznom formáte.

3.2.5 *Návrh rozhrania aplikácie*

Aplikácia bude rozdelená do niekoľkých častí, pričom tie najhlavnejšie budú menu, pomocou ktorého sa bude môcť používateľ navigovať a hlavná časť slúžiaca na zobrazovanie výstupov jednotlivých analýz a komunikáciu s používateľom prostredníctvom rôznych formulárov. Po naštartovaní systému z „live“ CD disku a spustení prostredia aplikácie bude používateľovi k dispozícii položka menu prostredníctvom, ktorej má možnosť pripojiť USB zariadenie a následne na toto zariadenie vytvoriť obraz súborového systému určeného na preskúmanie. Taktiež bude dostupná možnosť analyzovať obraz už vopred vytvorený a uložený na niektorom zariadení daného počítača.

Po vybratí daného obrazu, ktorý chceme analyzovať bude dostupné menu, ktoré bude poskytovať rôzne typy procedúr – analýz, ktoré budú na obrazovku zobrazovať jednotlivé výstupy spracované v prehľadnej forme. Pričom priebežne sa budú tieto výstupy archivovať, aby boli dostupné k prezretiu kedykoľvek počas spustenia danej aplikácie. Tieto výstupy analýz bude takisto možné uložiť do externých súborov na niektoré dostupné zariadenie v počítači, či už pevný disk, pripojený USB kľúč alebo podobne. Aplikácia bude takisto podporovať spúšťanie samostatných príkazov z kolekcia nástrojov „The Sleuth Kit“, ktorých výstup bude zobrazovať v hlavnej časti obrazovky.

Pred ukončením aplikácie bude užívateľovi dostupné bezpečné odpojenie predtým pripojeného USB zariadenia.

4 Implementácia

4.1 Výber implementačného jazyka

V pôvodnej špecifikácií bol uvedený programovací jazyk JAVA, ako nástroj na implementáciu výsledného produktu, no v návrhu riešenia sme prešli na kombináciu značkovacieho jazyka HTML a skriptovacieho jazyka PHP. Dôvody boli čisto praktické, neskúsenosť s jazykom JAVA, resp. neskúsenosť s používaním SWINGU ako vizualizačného prostredia pre program by viedli k značnému časovému zaneprázdňovaniu zbytočnými vecami.

4.2 Opis realizácie

V implementovanom integračnom prostredí sú použité nástroje programového balíka The Sleuth Kit, pričom v rámci navrhovaných rutín forenznej analýzy sú niektoré z nástrojov skombinované tak, aby dávali požadovaný výsledok.

4.2.1 *Implementácia navrhovaných ruín*

Typy súborov

V rámci tejto rutiny sa používa nástroj sorter, ktorý zanalyzuje zadaný obraz disku a jeho výstupom sú informácie týkajúce sa typov súborov. Konkrétne sa použije príkaz *sorter –h –m ./mnt –d directory image*, ktorý do zadaného adresára directory vygeneruje html súbory s výstupmi k jednotlivým typom súborov, ktoré sú zároveň aj výstupmi nášho integračného prostredia.

Systém súborov

Pri tejto rutine sa robí analýza súborového systému obrazu disku. Na to sa používa nástroj fls, ktorý vypíše obsah adresára špecifikovaného i-uzlom. Konkrétne sa používa *fls –la image inode*, ktorého výstupom je dlhý formát výpisu (informácie o čase modifikácie, veľkosti, UID, ...) spolu s vypísaním aj adresárov ./ a ../ . Výstup je následne spracovaný parsovacou funkciou, ktorá z neho vyselektuje jednotlivé informácie a tieto sú následne poskytnuté používateľovi v prehľadnej forme.

Vymazané súbory

Táto časť analýzy je podobná ako systém súborov ale na rozdiel od nej sú jej výstupom iba vymazané súbory. Použije sa na to príkaz *fls –rd image*, ktorý rekurzívne prehľadáva celý image a vypíše iba vymazané súbory.

Timeline

Ide o jednu z analýz, ktorá si vyžaduje použitie viacerých nástrojov a to fls, ils a mactime. V prvom rade sa použije nástroj fls, konkrétne *fls –r –m ./mnt image >> subor*, ktorý rekurzívne prehľadá celý obraz disku a výstup so záznamami o nájdených súboroch a adresároch presmeruje do zadaného súboru. Následne na to sa použije nástroj ils, ktorý vypisuje informácie o jednotlivých i-uzloch. Použije sa príkaz *ils –m image >> subor* a jeho výstup je takisto presmerovaný do toho istého súboru. Nakoniec sa použije nástroj mactime, ktorý z výstupov príkazov fls a ils vytvorí časovú líniu práce so súbormi na obraze disku. Použije sa *mactime –b subor –i hour subor.sum*, ktorý ako parameter preberá súbor s výstupmi nástrojov fls a ils, parameter –i hour určuje zameranie na zmeny v časových jednotkách hodín. Výstup je poskytnutý používateľovi v prehľadnej forme.

Informácie o i-uzloch

Výsledkom tejto analýzy sú podrobnejšie informácie o jednotlivých i-uzloch. Pre výpis všetkých i-uzlov sa používa nástroj ils – *ils –e image*, ktorý vypíše všetky alokované aj nealokované i-uzly a jeho výstup je následne spracovaný do prijatelnejšej formy. Na výpis informácii o konkrétnom i-uzle sa používajú nástroje ffind, icat v kombinácii s file a istat. Príkaz *ffind –a image inode*, poskytuje informácie o súboroch resp. adresároch ukazujúcich na daný i-uzol. Výstupom príkazu *icat image inode | file –z –b* – je typ daného i-uzla. Nakoniec príkaz *istat image inode* poskytuje detailné informácie o zadanom i-uzle. Výstupy všetkých nástrojov sú postupne spracované a prezentované používateľovi.

Informácie o blokoch (fragmentoch)

V rámci tejto analýzy sa používajú dva nástroje. Prvý dls na vypísanie všetkých alokovaných aj nealokovaných blokov na obraze disku a to vo forme *dls –elb image*. Druhý nástroj dcat sa používa na vypísanie obsahu konkrétneho fragmentu pričom sa používajú tri rôzne spôsoby výpisu. Na vypísanie obsahu vo forme ASCII znakov slúži príkaz *dcat –a image fragment* . Na hexadecimálny výpis obsahu sa použije ten istý príkaz ale s prepínačom *–h*. Nakoniec sa na výpis obsahu vo forme ASCII reťazcov použije výstup príkazu dcat v kombinácii s nástrojom srch_strings, *dcat –a image fragment | srch_strings –a*.

Informácie o obraze disku

V rámci tejto analýzy sa používa nástroj fsstat, ktorý vypíše detailné informácie týkajúce sa vlastností analyzovaného obrazu disku.

4.2.2 *Implementácia ostatných funkčných častí aplikácie*

Vytváranie záznamov

Pre uchovanie výstupov jednotlivých analýz je používateľovi poskytnutá možnosť uloženia výsledkov. Tieto sa v priebehu vykonávania jednotlivých rutín uchovávajú do dočasných súborov, ktoré budú v prípade potreby prekopírované do zadaného adresára.

Vytvorenie image disku

Používateľ má možnosť vytvárať image práve namontovaných diskov (súborových systémov).

Pri vytváraní image disku program vytvorí zoznam namontovaných súborových systémov. Používateľ má možnosť vybrať jeden z nich pomocou kombo boxu. Okrem toho je nutné zadať umiestnenie, kam má byť nový image disku vytvorený.

Pri práci program využíva príkaz *dd -if="input file" -of="output file"*.

Pripojenie USB disku

Program na začiatku vytvorí zoznam pripojených usb zariadení. Po vybratí a potvrdení namontuje zariadnenie príkazom *mount /dev/vybrane_usb /mnt/vybrane_usb* k adresaru /mnt/vybrane_usb. Po skončení príkazu mount program overí, či bol usb disk úspešne namontovaný a výsledok oznámi používateľovi.

Odpojenie USB disku

Program na začiatku vytvorí zoznam namontovaných usb zariadení. Po vybratí a potvrdení odmontuje zariadnenie príkazom u*mount vybrane_usb*. Po skončení príkazu umount program overí, či bol usb disk úspešne odmontovaný a výsledok oznámi používateľovi.

4.2.3 *Implementácia okna aplikácie*

Na implementáciu integračného prostredia sme najskôr navrhovali programovací jazyk JAVA, po podrobnejšom premyslení a zvážení výhod, t.j. jednoduchosti, lepším možnostiam

pri editovaní sme sa ubrali smerom k programovaciemu jazyku PHP a JavaScript ktorými sme vytvárali stránky a obsah integračného prostredia v jazyku HTML.

Ako základ narábania s podstránkami sme si zvolili pomerne novú technológiu asynchrónnych požiadaviek na url adresy AJAX, túto technológiu sme si zvolili z nasledujúcich dôvodov. Stránka je graficky vytvorená z viacerých obrázkov ktoré by bolo pri každom znova načítavaní obsahu stránky reloadovať, pri niektorých analyzujúcich programoch, ktoré potrebujú viac výpočtového času príslušného počítača by nastal efekt niekoľko sekundového okna bez niektorých obrázkov a obsahu, tomuto sme zabránili nasadeniu technológie AJAX, ktorou načítavame iba potrebný obsah a vyhýbame sa znova načítavaniu obrázkov.

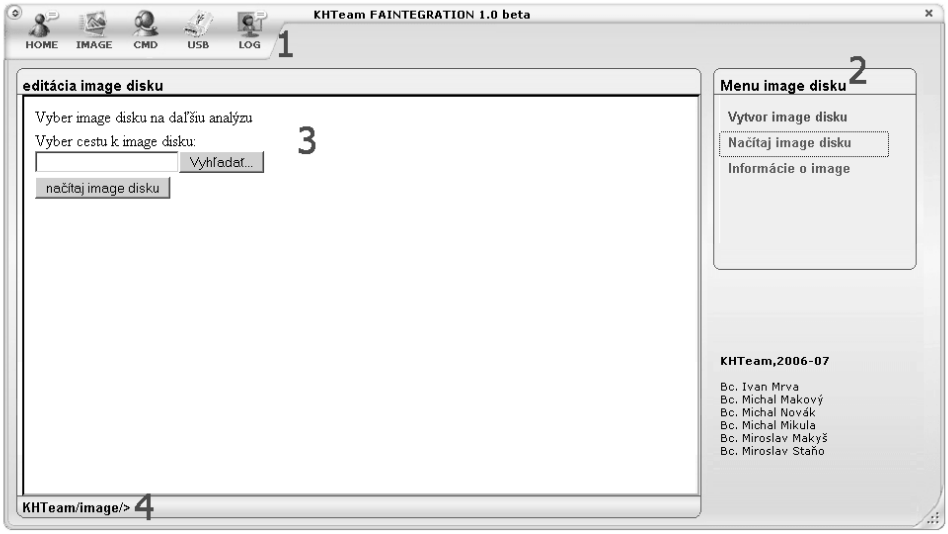
Základom stránky aplikácie je niekoľko samostatných celkov, nimi sú ako vidno na obrázku 1:

hlavné menu programu

menu k jednotlivým položkám hlavného menu

hlavné okno aplikácie

príkazový riadok



Obr.1 Hlavné okno aplikácie

Hlavné menu je robené ako klasický odkaz na index.php s pomocnou premennou sub, ktorá definuje aké pod menu a iné časti stránky budú načítané pri kliknutí na tú ktorú položku. Načítavanie prebieha klasicky reloadom stránky.

Po načítaní stránky je k dispozícií bočné pod menu, ktoré je vytvorené pomocou kaskádových štýlov a pomocných JavaScript skriptov. Pri kliknutí na daný odkaz sa zavolá nami definovaná JavaScript funkcia ktorá na základe vstupných premenných vytvorí http

request a zavolá príslušnú url ktorej výstup bude tvoriť obsah danej položky pod menu. Vygenerovaný obsah sa vloží hlavného okna aplikácie ktoré je tvorené plávajúcim IFRAME definovanom v jazyku HTML. Pomocou JavaScript funkcií smerujeme jednotlivé výstupy do daných oblastí stránky ktoré sú definované a určované parametrom ID v HTML tágu. Funkciou document.getElementById('Id') si zachytím objekt oblasti na stránke a metódou innerHTML tam vyplním obsah generovaný príslušne zavolaným PHP skriptom.

V spodnej lište ja umiestnený príkazový riadok, ktorým si možno volať ľubovoľný príkaz spustiteľný z klasického príkazového riadku shellu na danom systéme, táto možnosť má napomôcť skúsenému užívateľovi, ktorý vykonáva forenznu analýzu napadnutého stroja volať aj ďalšie funkcie a príkazy, ktoré nie sú priamo implementované v integračnom prostredí. Pri každom znova načítaní stránky je kurzor default ne umiestený v inpute príkazového riadku, táto vec je zabezpečená vlastnosťou tágu body, a to tou že pri načítavaní stránky nastaví funkcia JavaScriptu kurzor na určený objekt v dokumente.

Implementácia stránky vychádzala z návrhu a špecifikácie produktu s pred implementácie a dodatočným pozmenením niektorých navrhovaných vlastností a funkcionalít, v celku hodnotím implementovanie ako hladko prebiehajúci postup, pri ktorom sme narazili na niekoľko menších nezrovnalostí, ale ako tím sme ich vyriešili a priviedli produkt do záverečnej, takmer hotovej verzie pre nasadenie do praxe.

5 Overenie riešenia

5.1 Postup pri testovaní

Pri testovaní sme testovali každú funkciu zvlášť a to takým spôsobom, aby nami vytvorené funkcie prebehli všetkými vetvami (prípad úspechu, neúspechu, viac možností výsledku).

5.2 Výsledky

Funkcia	Testovaná vlastnos funkcie	Výsledok
vytvorene image disku	Načítali sa všetky disky podľa očakávania?	áno
	Bol image disku úspešne vytvorený na očakávanom mieste a so zvoleným diskom?	áno
načítanie image disku	Bola nastavená cesta image disku podľa očakávania?	áno
informácie o image disku	Zobrazili sa všetky požadované informácie?	áno
pripoj USB	Boli načítane všetky pripojene USB disky podľa očakávania?	áno
	Bol vybraný USB disk úspešne namontovaný na vybrané miesto?	áno
	Funguje správne testovanie namontovania USB disku?	áno
odpoj USB	Boli načítané všetky namontované USB disky podľa očakávania?	áno
	Bol vybraný USB disk úspešne odmontovaný?	áno
	Funguje správne testovanie odmontovania USB disku?	áno
zobrazenie výsledkov	Pracujú všetky funkcie používane na analyzovanie image disku správne a zobrazujú očakávané výsledky?	áno
	Pracujú správne všetky ošetrenia výnimočných situácii?	áno
uloženie výsledkov	Sú získané výsledky uložene na požadované miesto v požadovanom formáte?	áno
	Sú uložene všetky výsledky?	áno

6 Zhodnotenie

Práca na projekte vykonaná v letnom semestri 2006/2007 sa skladala z niekoľkých fáz. V prvej som konkrétne navrhovali jednotlivé časti systému, v ďalšej sme vytvárali "holú" aplikáciu bez žiadnej funkcionality a v konečnej fáze sme integrovali, resp. implementovali logiku testov a dosiahnuté výsledky dokumentovali.

6.1 Čo sme nestihli

Pri implementácií integračného prostredia sme sa snažili dotvoriť všetky dopredu určené a zadané ciele, menšie nedostatky môžeme priznať v rozsahu a detailnosti záverečnej správy k projektu.

6.2 Čo sme sa naučili

Pri tvorení a spolupráci sme sa naučili okrem nových technických a programátorských záležitostí, pracovať v týme, čo často krát býval problém.

Príloha A – Systémová príručka

Systémová príručka obsahuje zoznam požiadaviek potrebných na spustenie výslednej aplikácie.

Keďže daná aplikácia je dodávaná na „bootovateľnom“ cd disku s operačným systémom Slax, ktorý v sebe zahŕňa všetky aplikácie potrebné na spustenie výslednej aplikácie slúžiacej na forenznu analýzu, odpadajú akékoľvek softvérové požiadavky nutné na spustenie aplikácie.

Jedinými požiadavkami zostávajú teda hardvérové požiadavky na počítač, na ktorom má byť táto aplikácia spustená.

Zoznam hardvérových požiadaviek je nasledovný:

IDE rozhraním pripojená CD-ROM mechanika,
schopnosť BIOS-u zaviesť systém z CD disku,
minimálne 144 MB operačnej pamäte RAM, lepšie však aspoň 256 MB RAM,
procesor i486 alebo vyšší – Pentium alebo AMD,
klávesnicu, resp. myš pripojenú prostredníctvom PS2 alebo USB rozhrania (myš pripojená na COM rozhranie nie je automaticky rozpoznaná, ale môže byť použitá).

Pevný disk nie je vyžadovaný, avšak na odkladanie dát získaných forenznou analýzou pomocou aplikácie je potrebný určitý odkladací priestor, či už pripojený IDE alebo USB rozhraním.

Príloha B – Uživátelská príručka

Používateľská príručka obsahuje návod na spustenie aplikácie a opis používateľského rozhrania aplikácie.

B.1 Spustenie aplikácie

Výsledný produkt je realizovaný ako webová aplikácia. Samotná aplikácia nevyžaduje na spustenie žiadnu inštaláciu. Je uložená na „bootovateľnom“ CD disku dodávaného v rámci výsledného produktu. Po vložení tohto CD disku naštartuje na danom počítači „live“ verzia operačného systému Slax, ktorý už obsahuje nainštalovaný web server Apache, internetový prehliadač a všetky ostatné náležitosti potrebné na spustenie aplikácie. Po naštartovaní operačného systému sa na obrazovke automaticky zobrazí úvodná obrazovka aplikácie slúžiacej na forenznu analýzu linuxového súborového systému.

Minimálnou a nutnou požiadavkou na spustenie tejto aplikácie je teda potreba zaviesť („nabootovať“) operačný systém z dodávaného CD disku.

B.2 Používateľské rozhranie

Používateľské rozhranie je prehľadné, jednoduché a intuitívne. Po naštartovaní operačného systému sa na obrazovke zobrazí úvodná stránka aplikácie. Táto stránka je rozdelená do niekoľkých význačných častí:

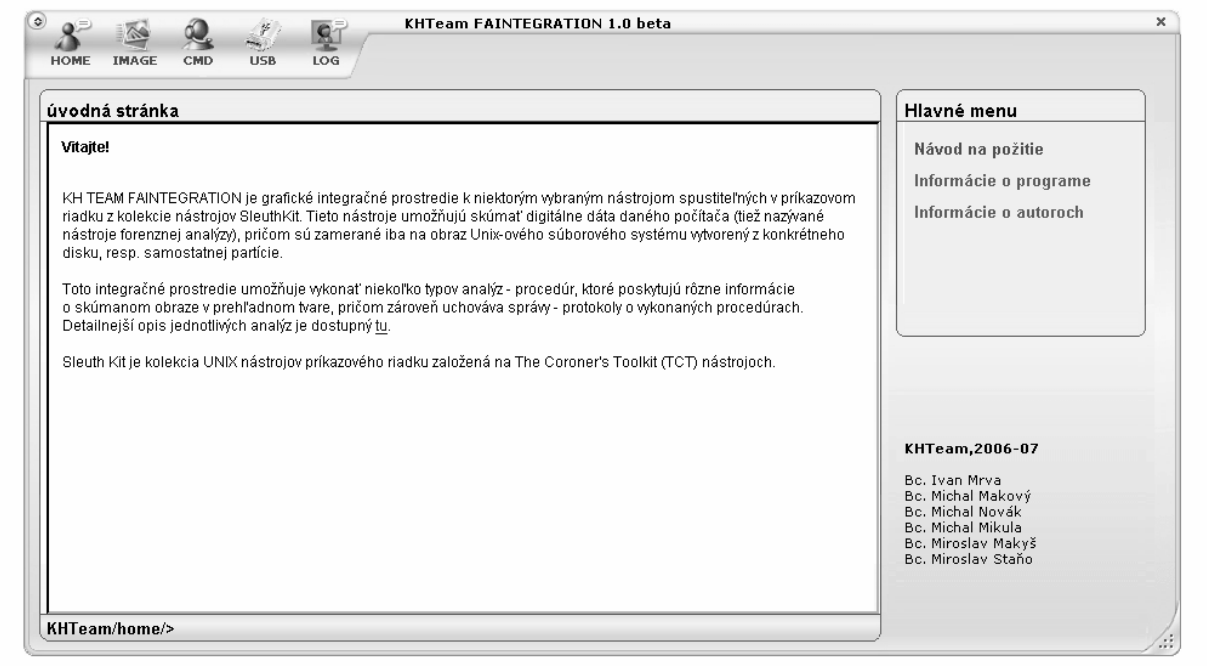
názov aplikácie – zobrazený v hornej časti v strede,

hlavné menu – umiestnené vľavo hore,

vedľajšie menu prislúchajúce výberu z hlavného menu - zobrazené napravo,

hlavná časť stránky slúžiaca na zobrazenie informácií prislúchajúcim jednotlivým položkám hlavného a vedľajšieho menu – umiestnená naľavo od vedľajšieho menu, pokrývajúca najväčšiu časť obrazovky,

príkazový riadok – umiestený v spodnej časti obrazovky.



Obr. B-1 Používateľské rozhranie webovej prezentácie – úvodná obrazovka.

Používateľ obsluhuje stránku prostredníctvom hlavného alebo vedľajšieho menu, ktoré sú rozdelené do viacero položiek alebo pomocou príkazového riadku.

B.2.1 Hlavné menu

Hlavné menu obsahuje nasledovné položky:

„HOME“ (Domov) – odkaz na úvodnú stránku,

„IMAGE“ (Obraz súborového systému) – odkaz na stránku slúžiacu na základnú prácu s obrazom súborového systému,

„CMD“ (Nástroje forenznej analýzy) – odkaz na stránku, ktorá poskytuje používanie jednotlivých nástrojov forenznej analýzy na danom obraze súborového systému,

„USB“ (USB disk) – odkaz na stránku slúžiacu na pripojenie USB disku k danému počítaču,

„LOG“ (Správy o forenznej analýze) – odkaz na stránku s výsledkami - protokolmi o vykonanej forenznej analýzy.

B.2.1.1 Menu „HOME“

Po kliknutí na menu Domov sa v hlavnej časti stránky zobrazia úvodné informácie k aplikácii a vedľajšie menu obsahuje tri nasledujúce položky:

Návod na použitie – obsahuje informácie o tom ako používať túto aplikáciu (vlastne obsah tohto dokumentu).

Informácie o programe – zobrazí informácie o tejto aplikácii – prečo a za akým účelom bola vytvorená spolu s dátumom vytvorenia.

Informácie o autoroch – zobrazí informácie o tvorcoch aplikácie.

B.2.1.2 Menu „IMAGE“

Prostredníctvom tohto menu môže používateľ pracovať s obrazom súborového systému. Vedľajšie menu mu ponúka nasledovné možnosti:

Vytvorenie obrazu – zobrazí v hlavnej časti formulár prostredníctvom, ktorého je možné zo zariadenia pripojeného k počítaču (napr. USB kľúč, pevný disk) vytvoriť obraz tohto zariadenia, ktorý sa uloží na iné zariadenie pripojené k počítaču.

Načítanie obrazu – túto voľbu užívateľ zvolí vtedy, ak namiesto vytvorenia obrazu bude chcieť analyzovať obraz disku, ktorý je už vytvorený a uložený na niektorom zo zariadení pripojených na disku.

Informácie o obraze – zobrazí v hlavnej časti stránky informácie získané z načítaného, resp. vytvoreného obrazu disku a to napr. typ súborového systému, informácie o súborových blokoch a im prislúchajúcim číslam „i-uzlov", atď.

B.2.1.3 Menu „CMD“

Táto položka menu slúži na vykonávanie jednotlivých príkazov forenznej analýzy na danom obraze disku (resp. partície).

Ponúka nasledovné možnosti:

Spúšťanie analýz – rozbaľovacie menu, prostredníctvom ktorého je možné zvoliť typ analýzy, ktorý chceme na načítaný obraz aplikovať. Je možné vykonať nasledovné rutiny:

Typy súborov,

Súborový systém,

Vymazané súbory,

Časové línie súborov,

Meta dáta,

Dátové jednotky.

Výsledky týchto rutín sa zobrazia v hlavnej časti stránky.

Informácie o analýzach – tento odkaz zobrazí v hlavnej časti stránky detailnejšie informácie o výsledkoch vyššie spomenutých typoch analýz.

B.2.1.4 Menu „USB“

Prostredníctvom tohto menu je umožnené používateľovi pripojiť k danému počítaču USB disk, ktorý je možné následne používať ako úložisko dát pre výsledky forenznej analýzy alebo úložisko pre vytvorený obraz disku, atď. Tento disk je takisto možné aj bezpečne odpojiť.

Vedľajšie menu obsahuje dve položky a to:

Pripojenie USB disku – zobrazí jednoduchý formulár, prostredníctvom, ktorého je možné pripojiť k systému USB disk.

Odpojenie USB disku – zobrazí formulár slúžiaci na bezpečné odobratie zariadenia zo systému.

B.2.1.5 Menu „LOG“

Prostredníctvom tohto menu môže používateľ pracovať s výsledkami jeho doterajších analýz, môže ich prezerať alebo ich ukladať do súborov.

Možnosti vedľajšieho menu sú nasledujúce:

Zobrazenie výsledkov – rozbaľovacie menu, ktoré ponúka tieto možnosti:

Všetky analýzy – zobrazí v hlavnej časti za sebou usporiadané výsledky všetkých doteraz spustených analýz na danom obraze súborového systému.

Analýza 1

Analýza 2

…

…

Analýza N – táto a predchádzajúce položky zobrazia výsledok iba konkrétnej analýzy, napr. analýzy č. 1, 2 alebo N.

Uloženie výsledkov – zobrazí formulár, pomocou ktorého je možné všetky zozbierané výsledky doteraz aplikovaných rutín uložiť do súborov na disk alebo iné dostupné úložisko dát pripojené k počítaču.

B.2.2 Príkazový riadok

Príkazový riadok je špeciálna časť stránky zobrazená úplne v spodnej časti pripomínajúca stavový riadok. Funkciou tejto časti stránky je možnosť do neho vpisovať rôzne príkazy, ktoré sa nachádzajú v kolekcii nástrojov „The Sleuth Kit“. Táto možnosť je

vhodná napr. pre pokročilých používateľov, ktorí sú s nástrojmi „The Sleuth Kit" už oboznámení, pretože im napr. ponúka možnosť použiť nástroj, ktorý nebol použitý v žiadnej z poskytovaných rutín. Výstup tohto príkazu sa zobrazí v hlavnej časti obrazovky, avšak v nesformátovanom tvare, aký by bol po spustení v konzole operačného systému.