UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Aljaž Bratkovič

PREPREČEVANJE IZPADA IN ZAGOTAVLJANJE VARNOSTI JAVNIH RAČUNALNIŠKIH SISTEMOV

DIPLOMSKO DELO VISOKOŠOLSKEGA STROKOVNEGA ŠTUDIJA

Mentor: doc. dr. Tomaž Dobravec

Ljubljana, 2009

Univerza
v Ljubljani

Fakulteta za računalništvo
in informatiko

Tržaška 25
1000 Ljubljana, Slovenija
telefon: 01 476 84 11
faks: 01 426 46 47
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 00416/2008
Datum: 15.10.2008

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **ALJAŽ BRATKOVIČ**

Naslov: **PREPREČEVANJE IZPADA IN ZAGOTAVLJANJE VARNOSTI JAVNIH RAČUNALNIŠKIH SISTEMOV**

PREVENTING DOWNTIME AND ENSURING SAFETY FOR PUBLIC ACCESS COMPUTERS

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija

Tematika naloge:

V diplomskem delu preglejte, preizkusite in ovrednotite delovanje strojne in programske opreme namenjene preprečevanju izpadov in zagotavljanju varnosti javnih računalniških sistemov. Osredotočite se na vodilne komercialne rešitve na tem področju. Ugotovite katere med njimi so najprimernejše za različne oblike javnih računalniških sistemov (knjižnice, šole, fakultete, internetne kavarne in podobno).

Izdelajte tudi lastno rešitev za omenjen problem. Pri tem uporabite odprtokodno programsko opremo in neplačljiv operacijski sistem. Izdelajte aplikacijo, ki bo namenjena širšemu krogu uporabnikov. Aplikacija naj bo dovolj preprosta, da jo bodo lahko uporabljali zaposleni v izobraževalnih ustanovah, brez pomoči administratorjev in ne glede na operacijski sistem in strojno opremo, ki se v ustanovi uporablja.

Mentor:
doc. dr. Tomaž Dobravec

Fakulteta za računalništvo in informatiko
2
UNIVERZA V LJUBLJANI

Dekan:
prof. dr. Franc Solina

I Z J A V A O A V T O R S T V U

diplomskega dela

Spodaj podpisani/-a Aljaž Bratkovič,

z vpisno številko 63010015,

sem avtor/-ica diplomskega dela z naslovom:

Preprečevanje izpada in zagotavljanje varnosti javnih računalniških sistemov

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal/-a samostojno pod mentorstvom (naziv, ime in priimek)

  doc. dr. Tomaž Dobravec

  in somentorstvom (naziv, ime in priimek)

  _____

- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela

- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki »Dela FRI«.

V Ljubljani, dne _____ Podpis avtorja/-ice: _____

ZAHVALA

V prvi vrsti gre zahvala družini, predvsem staršem in bratu, ki so mi ne samo v času študija, ampak že od malih nog stali ob strani in me spodbujali. Rad bi se zahvalil tudi dr. Dobravcu za vso pomoč pri vsebinskem in tehničnem delu diplomske naloge. Knjižnici Bežigrad, Janezu, Iztoku ter Elvisu se zahvaljujem za programsko in strojno opremo, brez katere diplomske naloge ne bi mogel izdelati. Hvala tudi vsem sošolcem in prijateljem, ki so v času študija kakorkoli prispevali k izdelku, ki ga vidite pred sabo. Na koncu bi se zahvalil še Jasni, za vse...

SEZNAM UPORABLJENIH KRATIC IN SIMBOLOV

CD	Compact Disk
CDP	Continuous Data Protection
LUN	Logical Unit Number
FAT	File Allocation Table
BIOS	Basic Input Output System
POST	Power On Self Test
IP	Internet Protocol
LAN	Local Area Network
WAN	Wide Area Network
TCP/IP	Transmision Control Protocol / Internet Protocol
DHCP	Dynamic Host Configuration Protocol
NTFS	Windows NT File System
SUS	Software Update Services
WSUS	Windows Server Update Services
UDP	User Datagram Protocol
DNS	Domain Name Server
B	Byte
GB	Giga Byte
FTP	File Transfer Protocol
TFTP	Trivial File Transfer Protocol
GRUB	Grand Unified Bootloader
IDE	Integrated Drive Electronics
SATA	Serial AT Attachment
BOOTP	Bootstrap Protocol
ROM	Read-Only Memory
MBR	Master Boot Record
VBR	Volume Boot Record
LILO	Linux Loader
NTLDR	NT Loader

POVZETEK

PREPREČEVANJE IZPADA IN ZAGOTAVLJANJE VARNOSTI JAVNIH RAČUNALNIŠKIH SISTEMOV

Diplomska naloga obravnava načine preprečevanja izpadov in zagotavljanja varnosti javnih računalniških sistemov. Osrednji del naloge sestavlja več podpoglavij. Prvo je namenjeno opisu splošnih pojmov, kot so kloniranje trdega diska, ustvarjanje slike trdega diska in njegov posnetek, ki skušajo bralcu predstaviti področje ter ga uvesti v terminologijo, potrebno za njegovo razumevanje. Naslednje poglavje je posvečeno preizkusom vodilnih strojnih ter programskih rešitev, namenjenih preprečevanju izpada in zagotavljanju varnosti javnih računalniških sistemov. Vsebuje natančen opis namestitve, vzdrževanja in dela s strojnimi (varnostne kartice) in programskimi rešitvami (Deep Freeze, Norton Ghost). Ključni namen je kar najbolj posnemati realno okolje, v katerem naj bi se omenjena strojna in programska oprema pojavljala in jo v tem okolju tudi preizkusiti. Sledi poglavje, katerega namen je ustvariti možno rešitev za preprečevanje izpada in zagotavljanje varnosti javnih računalniških sistemov. Le-ta temelji na odprtokodnih programih (nalagalnik GRUB, dd) in storitvah (TFTP) ter operacijskem sistemu Linux. Uporabnik lahko omenjeno rešitev uporablja brez razumevanja njenega delovanja, saj ponuja preprost način obnavljanja trdega diska računalnika, s tem pa tudi preprečevanje izpada in zagotavljanja varnosti. V ta namen rešitev deluje tudi na računalnikih z nameščenim operacijskim sistemom, ki ni distribucija Linux, saj uporablja postopek mrežnega zagona. S tem postopkom se zagotovi, da računalnik po zagonu začne z izvajanjem skripte, napisane v lupini Bash, ki omogoča pisanje slike diska iz naprave oziroma na njo. V zaključku so opisane prednosti in pomanjkljivosti vseh preizkušenih programov, strojne opreme, opisane izvedene rešitve ter njihova primerjava.

Ključne besede: *slika trdega diska, kloniranje trdega diska, strojna oprema, programska oprema, operacijski sistem Linux*

PREVENTING DOWNTIME AND ENSURING SAFETY FOR PUBLIC ACCESS COMPUTERS

Thesis deals with ways of preventing downtime and ensuring safety for public access computer systems. Its main part consists of several subsections. The first is devoted to the description of general concepts, such as cloning the hard disk, creating an image of hard disks and hard disk snapshots, which goal is to present and introduce the terminology necessary for understanding to the reader. The next section is devoted to testing the leading hardware and software solutions aimed at the prevention of downtime and ensuring safety for public computer systems. It contains a detailed description of installation, maintenance and working with hardware (security card) and software solutions (Deep Freeze, Norton Ghost). The key aim is to emulate the most realistic environment in which hardware and software solutions are applied and testing the solutions in that environment. Next section describes a possible solution to prevent downtime and ensuring security for public computer systems. It is based on open source programs (GRUB loader, dd), services (TFTP) and Linux operating system. The user can use that solution without understanding its structure because it offers a simple way of restoring a computer hard drive, as well as downtime prevention. This solution works even on computers that do not have a Linux distribution installed, because it uses the process of network booting. This process ensures that after a reboot, computer begins running a Bash script, which allows writing disk images from or on to the device. The conclusion describes the advantages and disadvantages of all the tested software, hardware implemented solutions, and describes their comparison.

Key words: *hard disk image, hard disk cloning, software, hardware, Linux operating system*

KAZALO

1. UVOD

Zamisel za to diplomsko delo je nastala med mojim praktičnim izobraževanjem, ki je potekalo v eni od ljubljanskih knjižnic, Knjižnici Bežigrad. Ena izmed mojih nalog je bila skrb za računalniške sisteme, namenjene uporabnikom knjižnice. Računalnike, ki so javno dostopni, je bilo treba ustrezno zaščititi pred neveščimi, zlonamernimi ali samo nespretnimi obiskovalci. Hitro se namreč zgodi, da uporabnik ob nameščanju programske opreme, ki jo potrebuje za delo, v sistemu naredi tudi spremembe, ki niso dobrodošle. Prav tako lahko uporabnik že z branjem e-maila ali preprostimi prenosi določenih datotek na sistem vpliva slabo. To se odraža v času nedelovanja računalniškega sistema, to je v času, ko računalnik ni na voljo oz. ne deluje (*angl. downtime*).

V ta namen se v omenjeni ustanovi uporabljajo varnostne kartice, ki zagotavljajo, da se računalnik po ponovnem zagonu povrne v stanje, ki smo ga predhodno določili. Tako se na računalniku ne poznajo nobene spremembe, ki jih je uporabnik naredil (nameščanje programske opreme, posnete datoteke), hkrati pa je računalnik varen pred virusi, črvi in drugo zlonamerno kodo. Ob spoznavanju delovanja in značilnosti varnostnih kartic se mi je porajalo vprašanje, kako s čim manj napora obvladovati neželeno spreminjanje značilnosti računalniškega sistema. Pri raziskovanju te teme nisem imel na voljo knjižne literature, največ podatkov sem našel na spletu.

Kot bom v nadaljevanju predstavil, varnostne kartice sicer zelo dobro opravljajo svojo nalogo, vendar pa imajo pomanjkljivost, da je treba vsako posamezno kartico ročno vstaviti v računalnik, jo namestiti in pripraviti na vsakem računalniku posebej. Tako sem začel spoznavati tudi programsko opremo, ki je namenjena »javnim« računalnikom. Spoznal sem, da imajo programske različice celo določene prednosti, saj so bile razvite z mislijo, kako administratorju sistema omogočiti delo na daljavo. Ob raziskovanju značilnosti in uporabnosti programske opreme sem ugotovil, da je temeljna tehnologija tako programske opreme kot tudi varnostnih kartic tako imenovani posnetek (*angl. snapshot*) trdega diska. Od tu pa sem svoje delo nadaljeval v smeri odprtokodne, prostodostopne implementacije varnostnega sistema za javne računalnike.

Kot cilj sem si zadal izdelati sistem, ki bi temeljil na operacijskem sistemu Linux (kot odprtokodni, neplačljivi operacijski sistem). Le-ta omogoča prenos shranjene slike (*angl. image*) pomnilne naprave s strežnika na ciljni računalnik s pomočjo zagonskega pomnilnega medija (disketa, CD-ROM). Tak način se mi je zdel smiseln zato, ker se večino dela lahko opravi na strežniku, poleg tega pa ima še nekaj drugih prednosti, ki jih omenjam v nadaljevanju naloge. Takšno rešitev bi lahko uporabljali v primeru, ko računalnik odpove in je treba nanj hitro prenesti sliko delujočega računalniškega sistema. Takšna slika mora biti dovolj majhna, da se omogoči hiter prenos. Poleg tega je dobro imeti tudi hitro povezavo med strežnikom in ciljnimi računalniki ter novejšo strojno opremo, predvsem trdi disk. Druga uporabna vrednost takšnega sistema bi lahko bila v primeru, ko je treba v kratkem času zagotoviti namestitev operacijskih sistemov na več računalnikih (na primer po nakupu novih računalnikov). Tako lahko namestimo operacijski sistem in drugo programsko opremo na enem računalniku, naredimo sliko tega računalnika in jo pošljemo na strežnik. Odtod jo potem lahko pošljemo na želene ciljne računalnike.

2. PREPREČEVANJE IZPADA IN ZAGOTAVLJANJE VARNOSTI JAVNIH RAČUNALNIŠKIH SISTEMOV

Preden bomo prešli na dejanske rešitve problema, naj na kratko opišem pojme in tehnologijo, ki se uporablja v namen preprečevanja časa izpada (*angl. downtime*) računalniškega sistema, lahko pa se uporablja tudi za vrsto drugih problemov.

2. 1. Splošno o slika trdega diska, kloniranju diska in snapshot tehnologiji

2. 1. 1. Image ali slika pomnilne naprave

Slika trdega diska (*angl. disk image*) je besedna zveza, ki opisuje kopiranje podatkov neke pomnilne naprave (največkrat trdega diska, lahko pa tudi prenosnega diska, CD-ROM-a in podobno) ter prenašanje teh podatkov na drugo podobno ali enako pomnilno napravo. V originalnem kontekstu se je beseda image nanašala na proces ustvarjanja podobe ali kopije določenega računalniškega trdega diska, vključno z operacijskim sistemom (če je bil ta na trdem disku prisoten), programsko opremo, ki je bila nanj nameščena, nastavitvami sistema in podatki. Slika je torej kopija trdega diska, shranjena v posebnem (kompresiranem ali skrčenem) formatu v obliki datoteke. Slika torej uporabniku omogoča, da z natančno kopijo računalniškega sistema in podatkov, shranjenih na njegovem trdem disku, kopira sistemske nastavitve za namestitev na drug računalnik ali pa to sliko premakne na drug trdi disk istega računalnika.

Večina ljudi v zvezi s sliko diska najprej pomisli na programsko opremo, ki zagotavlja hitro in enostavno ustvarjanje kopije izbranega diska in informacij, shranjenih na trdem disku. Ti ljudje pomislijo na sliko kot na redundanco podatkov (*angl. backup*) operacijskega sistema in programske opreme. Sliko lahko razumemo tudi, ali pa predvsem kot, podobo aktivnega, delujočega računalniškega sistema. To pa se izkaže za zelo uporabno v primerih, ko imamo probleme z računalniškim sistemom med njegovim delovanjem. S tem mislimo predvsem na napade virusov, črvov in druge zlonamerne kode. Med probleme lahko uvrstimo tudi napake v strojni opremi, programski opremi, napake pri inštalaciji programske opreme, sistemskih gonilnikov, ki povzročijo napake v sistemu, »človeške napake«, na primer med nameščanjem nove programske opreme in posodabljanjem obstoječe. Med neljube dogodke lahko uvrstimo tudi tako imenovane naravne katastrofe, kot so poplave in potresi. Vse te nevarnosti nas lahko privedejo do tega, da je treba trdi disk izbrisati ali formatirati, to pa lahko privede do izgube podatkov. Tako lahko sliko razumemo tudi kot »rešilno« kopijo diska, ki jo lahko uporabimo, ko je treba na novo postaviti računalniški sistem. Na ta način lahko računalnik postavimo nazaj v stanje, v kakršnem je bil v času, ko je bila slika ustvarjena. Prednost takšnega načina dela je v tem, da nam na okvarjenih računalnikih ni treba posebej nameščati želenega operacijskega sistema in programske opreme ali nastavljati želene konfiguracije sistema. Slika računalniškega sistema je tako lahko v veliko pomoč administratorjem ali vzdrževalcem računalniških sistemov, še posebej kadar morajo skrbeti za veliko število računalnikov, ki naj bi imeli enake nastavitve. Administratorjem ni treba zapravljati dragocenega časa s posamičnimi nastavitvami, saj imajo sliko delujočega sistema (in ne samo podatkov na disku!) lahko že vnaprej pripravljeno in jo samo prenesejo na ciljne računalnike [12].

2. 1. 2. Kloniranje trdega diska (pomnilne naprave)

Z besedno zvezo kloniranje diska (*angl. disk cloning*) razumemo predvsem skupino programske opreme, s katero kopiramo vsebino trdega diska nekega računalnika na drug trdi disk, ki je lahko na istem ali na drugem računalniku. Z besedno zvezo kloniranje diska se opisuje tudi postopek, s katerim vsebino nekega trdega diska prepišemo v sliko. Najpogostejši je primer, ko kopiramo vsebino prvega trdega diska v sliko, nato pa iz te datoteke prekopiramo vsebino na drug trdi disk. Ta procedura je uporabna, ko prenašamo vsebino trdega diska na večji disk. Ta skupina programske opreme pa je uporabna tudi za druge namene. Naj naštejem in opišem le tiste najpomembnejše in najbolj razširjene primere uporab:

- naloži in obnovi (*angl. Reboot and restore*),
- nastavitev novih računalniških sistemov,
- nadgradnja diska,
- varnostna kopija sistema (*angl. Full system backup*).

2. 1. 2. 1. Naloži in obnovi (Reboot and restore)

Naloži in obnovi je metoda, pri kateri se disk računalnika avtomatično vrne v določeno stanje, ki ga je treba pred tem ustrezno nastaviti. Pri tem se disk naloži iz tako imenovane glavne slike (*angl. master image*), ki mora biti v delujočem stanju in čista v smislu neželene zlonamerne programske kode. To metodo uporabljajo predvsem izobraževalne ustanove (šole, knjižnice, fakultete), nekatere internetne kavarne in podobno. Metoda je uporabna in razširjena predvsem zato, ker se na mestih, kjer so računalniki prosto dostopni, rado zgodi, da uporabniki, pogosto nevede, škodijo računalniškemu sistemu z inštalacijo programske opreme, prenosom, brisanjem datotek ali kakršnimkoli drugim posegom v računalniški sistem. V vseh teh primerih se je računalnik sposoben vrniti v delujoče stanje. Takšno vrnitev v delujoče stanje lahko izvedemo samo v primerih, ko računalniški sistem kaže znake okvare ali v rednih intervalih (na primer, ko ponovno poženemo sistem ali vsakokrat, ko se uporabnik odjavi) [2].

2. 1. 2. 2. Nastavitev novih računalniških sistemov

Kloniranje diska je uporabna metoda, kadar nameravamo programsko opremo namestiti na več računalnikov. S kloniranjem lahko privarčujemo veliko časa, saj nam ni treba nameščati operacijskega sistema in programske opreme na vsakem računalniškem sistemu posebej [2].

2. 1. 2. 3. Nadgradnja diska

Kloniranje diska se uporablja, ko želimo vsebino diska prenesti na novejši (največkrat večji, hitrejši, sposobnejši) trdi disk [2].

2. 1. 2. 4. Varnostna kopija sistema (Full system backup)

Uporabnik lahko naredi kopijo celotnega (delujočega!) računalniškega sistema, vključno z operacijskim sistemom, podatki in nameščeno programsko opremo [2].

2. 1. 3. Posnetek trdega diska (Snapshot)

Beseda posnetek (*angl. snapshot*) ima svoj izvor v fotografiji. Z njo opišemo trenutek v določenem času. Za analogijo si lahko predstavljamo primer, ko fotografiramo osebo, ki stoji na lestvi. V naslednjem trenutku se lahko zgodi, da ta oseba z lestve pade, vendar na fotografiji še vedno stoji na lestvi. Na nesrečo te osebe nimamo moči, da bi jo v resnici vrnili v trenutek, ko je še stala na lestvi.

Na področju informacijske tehnologije lahko z računalniškim diskom storimo prav to. Vse neželene spremembe trdega diska, ki se dogodijo po posnetku, lahko odpravimo. Računalnik lahko povrnemo v posneti trenutek pred spremembami. Posnetki trdega diska ponujajo prednosti pri več opravilih, kot so zagotavljanje varnostnih kopij sistema, obnovitev podatkov ali testiranje programske opreme. V vseh teh primerih je ključnega pomena skok na prejšnje stanje in nadaljevanje dela z delujočega, nespremenjenega sistema. Administrator sistema lahko tako ustvari posnetek računalniškega sistema v več stanjih, na katere se »zna« računalnik nato vrniti.

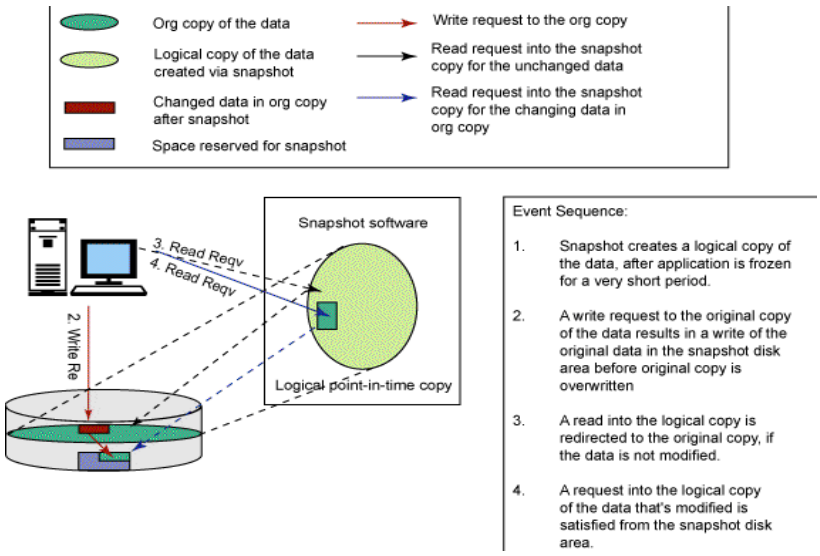
Pojma slika (kot stisnjena datoteka, ki pogosto vsebuje celotno sliko izbranega diska, vključno z operacijskim sistemom in uporabniško programsko opremo) in kloniranje (kot zapisovanje slike trdega diska na druge diske) lahko razumemo kot pojma, ki opisujeta določen proces, ali kot sinonim za skupino programske opreme, ki zgoraj povedano omogočata. Besedo posnetek pa lahko razumemo kot besedo, ki opisuje tehnologijo, s katero so implementirane nekatere različice programske in strojne opreme. Med njihove najbolj znane in razširjene različice spadajo izdelki, kot so Deep Freeze in pa Symantec Ghost (tudi na »klasično« sliko diska lahko gledamo kot na posnetek, saj posname stanje trdega diska v nekem času).

Poznanih je kar nekaj načinov implementacije posnetkov, med katerimi je najbolj znana slika. Različni proizvajalci programske in strojne opreme, namenjene posnetkom, uporabljajo različne pristope. Vsaka različica ima svoje prednosti in pomanjkljivosti. Nekaj najbolj znanih načinov izvedbe snapshot tehnologije so naslednji:

2. 1. 3. 1. Kopiraj pri pisanju (Copy-on-write)

Posnetek pomnilne naprave se ustvari na trdem disku v rezerviranem prostoru, do katerega ne dostopa nobena aplikacija ali operacijski sistem. Ko se posnetek prvič ustvari, se v njem shranijo le meta-podatki o tem, kje so originalni podatki. V času, ko posnetek nastane, se kopije fizičnih podatkov ne ustvarijo. Iz tega sledi, da se posnetek ustvari zelo hitro. Kopija posnetka nato sledi spremembam blokov (sekvenc bajtov in bitov z neko nominalno dolžino) na originalni pomnilni napravi, medtem ko se na njej izvaja pisanje. Originalni podatki, v katere se piše (oziroma dopisuje), se prekopirajo v preddoločen prostor za shranjevanje. Iz vsebine tega prostora za shranjevanje podatkov se ustvari posnetek, preden se originalni podatki prepišejo z novo vsebino. Tako je ta način dobil tudi ime copy-on-write ali kopiraj pri pisanju.

Preden je pisanje v blok podatkov dovoljeno, se originalni blok prestavi v pomnilni prostor za posnetek. Tako je zagotovljena identičnost med originalnimi podatki in posnetkom v času, v katerem je bil posnetek ustvarjen. Zahteva za branje iz prostora za posnetek nespremenjenih podatkov se preusmeri na originalno pomnilno napravo, torej na originalne podatke, medtem ko se zahteva za branje spremenjenih podatkov preusmeri na kopijo oziroma kopirane bloke podatkov v posnetku. Kot že rečeno, posnetek vsebuje meta-podatke, ki opisujejo bloke podatkov, ki so se spremenili od časa, ko je posnetek nastal. Originalni podatki se torej kopirajo v prostor za posnetek samo ob prvi zahtevi po pisanju.



Slika 1: Diagram opisuje operacijo snapshot, ki ustvari kopijo podatkov s pomočjo metode copy-on-write [8].

Metoda kopiraj pri pisanju pa ima lahko tudi negativen vpliv na obnašanje originalne pomnilne naprave. Ta negativni vpliv se pojavi zato, ker mora originalna pomnilna naprava počakati, da se originalni podatki prekopirajo v prostor, rezerviran za posnetek. Zahtevo za branje iz prostora za posnetek izpolni originalna pomnilna naprava v primeru, da se zahtevani podatki za branje niso spremenili. Ta metoda je dobra, saj zahteva malo prostora za nastanek posnetka, zato ker se v prostoru za posnetek hranijo le podatki, ki so se spremenili. Slaba stran pa je ta, da posnetek za delovanje potrebuje originalne kopije podatkov [8].

2. 1. 3. 2. Preusmeri pri pisanju (Re-direct on write)

Ta metoda je podobna prejšnji, vendar ni potrebno dvojno čakanje pri pisanju. Metoda je dobra, ker zahteva malo prostora na pomnilnem mediju in ker ponuja uporabne posnetke. Novo pisanje podatkov na originalno pomnilno napravo je preusmerjeno na drugo lokacijo – tisto, ki je rezervirana za posnetek. Prednost preusmeritve pisanja je v tem, da se izvrši le eno pisanje, medtem ko sta pri metodi kopiraj pri pisanju potrebni dve – prvo pisanje se izvrši, da se zapišejo originalni podatki, drugo pa, da se zapišejo spremenjeni podatki.

Pri metodi preusmeri pri pisanju originalni podatki vsebujejo kopijo podatkov v določenem času – posnetek, spremenjeni podatki pa se nahajajo v prostoru za posnetek. Ko je posnetek izbran za nalaganje, se morajo podatki v prostoru za posnetek prenesti nazaj na originalno pomnilno napravo. Če je bilo ustvarjenih več posnetkov, se postopki za dostop do originalnih podatkov, spremljanje podatkov v originalni pomnilni napravi in prostoru za posnetek kot tudi postopki za vzpostavitev sistema po brisanju posnetka zapletejo. Razlog za te zapletene postopke leži v tem, da posnetek potrebuje originalne podatke, originalni nabor podatkov pa lahko na originalni pomnilni napravi postane razdrobljen (*angl. defragmented*) [8].

2. 1. 3. 3. Razdeljeno okno (Split mirror)

Metoda razdeljeno okno ustvari fizično kopijo pomnilne naprave ali dela (particije) pomnilne naprave. Pri tem se lahko ustvari kopija, ki vsebuje datotečni sistem, celotno kopijo pomnilne naprave ali pa LUN[1] naprave, katere posnetek se ustvarja. Klon se lahko prenese na drugo pomnilno napravo, ki mora biti iste vrste in velikosti ali pa mora biti večja od originalne pomnilne naprave (mišljena velikost v B). Slabost tega načina je čas oziroma čakanje, saj se morajo vsi podatki iz ene pomnilne naprave ali enega njenega dela prenesti na drugo napravo oziroma njen drug del. To je tudi razlog, da posnetek ni dosegljiv takoj, v trenutku [8].

2. 1. 3. 4. Dnevniške datoteke datotečnega sistema (Log structure file architecture)

Ta rešitev uporablja dnevniške datoteke (*angl. log*), s katerimi sledi pisanju v originalno pomnilno napravo. Ko je treba obnoviti podatke oziroma nastavitve, se transakcije pisanj, ki so zabeležene v teh datotekah, izvedejo v obratni smeri [8].

2. 1. 3.5. Neprestana zaščita podatkov (Continuous data protection – CDP)

Metoda CDP, imenovana tudi continuous backup (neprestano varovanje, podvajanje), ustvari posnetek vsakič, ko se naredi sprememba v originalni pomnilni napravi. Posnetek spravi v rezervirani prostor na originalni pomnilni napravi. Metoda CDP ustvari datoteko, imenovano »elektronski dnevnik« vseh posnetkov originalne pomnilne naprave. Ta metoda se od prej opisanih razlikuje predvsem po značilnosti, da ustvari posnetek vedno, ko se zgodi sprememba podatkov na napravi. Ostale metode ustvarijo posnetek v določenem trenutku. CDP se uporablja predvsem za obnovitev objektov, kot so aplikacijski podatki (npr. večje baze podatkov) in datotek [8].

2. 2. Varnostne kartice

Sam sem se med vsemi koncepti preprečevanja izpada računalniškega sistema najprej srečal z varnostnimi karticami. Sledi kratek opis njihovega delovanja ter rokovanja oziroma dela z njimi.

Varnostne kartice so strojna oprema, ki omogoča avtomatično ustvarjanje tako imenovanih točk povratka sistema (*angl. restore points*). Administrator sistema lahko tako določi stanje, v katerega se je računalnik sposoben vrniti. Večina varnostnih kartic omogoča ustvarjanje več povratnih točk. To pomeni, da lahko administrator ustvari več povratnih točk in s tem prilagodi računalniški sistem več profilom uporabnikov. Hkrati pa lahko izkoristi to značilnost tudi za testiranje pravilnosti nove nameščene programske opreme.

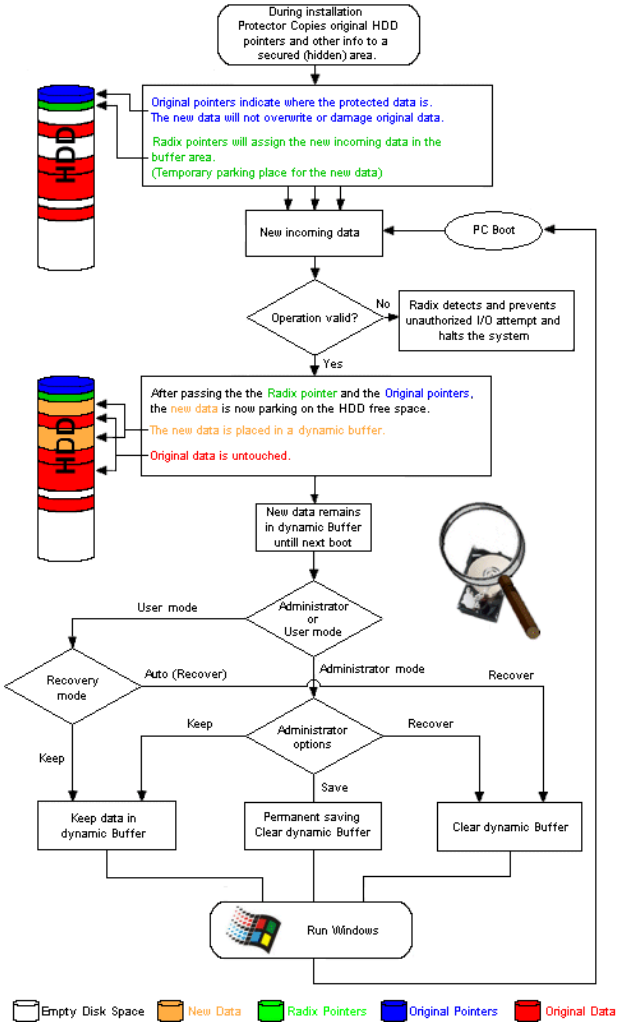
Varnostne kartice shranijo podatke, potrebne za obnovitev sistema, v določen (skrit ali varen) del trdega diska. Podatki zajemajo tako imenovano FAT (File Allocation Table) tabelo, tabelo particij trdega diska (*angl. partition table*) in osnovne BIOS nastavitve. Kartice ščitijo računalnik med njegovim zagonskim (*angl. boot up*) procesom tako, da se sistem ob zaznavi napake ali nepravilnosti vrne v želeno stanje. V tem primeru naloži sliko trdega diska, ki je

---

[1] Logical Unit Number je številka, dodeljena pomnilni napravi. Je entiteta SCSI protokola, ki se jo edino lahko naslavlja z dejanskimi vhodno/izhodnimi operacijami.

shranjena v posebnem prostoru – na trdem disku uporabljenega računalnika. Večina kartic namreč vsebuje vgrajene algoritme, ki preprečujejo, da bi se pisalo v tisti del trdega diska, ki »pripada« kartici. Med namestitvijo varnostne kartice se vsebina (kazalci do podatkov) trdega diska prekopira v varen del trdega diska. Originalni kazalci (*angl. pointers*) kažejo na vsebino, ki jo je treba zavarovati – kažejo stanje diska pred namestitvijo varnostne kartice. Algoritem, zapisan v kartici, poskrbi za nove kazalce, ki kažejo na nove datoteke v začasnem prostoru (*angl. buffer area*) za nove podatke. Ob vsakem ponovnem zagonu računalnika se pregleda stanje teh kazalcev in ob detekciji sprememb (tudi v BIOS-nastavitvah sistema) kartica operacijskemu sistemu prepreči zagon. S tem zavaruje poskuse zagona sistema iz drugih naprav, kot so recimo CD-ROM, zunanji trdi disk ali disketna enota. Prav tako se prepreči zagon sistemu, če imamo na računalniku veljavno namestitev kartice, kartico pa fizično odstranimo iz računalnika. Tako kartice zagotavljajo, da se zagon celotnega računalniškega sistema izvrši iz zaščitenega dela trdega diska. Če so vsi zgoraj omenjeni parametri (kartica na svojem mestu, BIOS-nastavitve) nespremenjeni, varnostna kartica po zagonu računalnika »pregleda« originalne kazalce in kazalce, ki kažejo v dinamični oziroma rezervirani del pomnilnika. Če so prisotne spremembe, spravi nove podatke v ustrezen del pomnilnika in jih obdrži do naslednjega zagona sistema.

Kartica ob zagonu podpira dva načina, in sicer: uporabniški način (*angl. user mode*) in administratorski način (*angl. manager mode*). Če je kartica v uporabniškem načinu, lahko izbiramo med možnostma Auto in Keep. Če izberemo možnost Auto, se del dinamičnega pomnilnika, v katerem so novonastali podatki, izprazni in operacijski sistem se naloži z izbrane oziroma ustvarjene točke povratka. Če izberemo opcijo Keep, se novonastali podatki obdržijo do naslednjega zagona sistema. Ta način je idealen, kadar je treba preizkusiti novo namestitev določene programske opreme ali posodobiti katerokoli programsko opremo ali operacijski sistem. Velikokrat se namreč zgodi, da ravno ob namestitvi nove programske opreme ali ob posodobitvi operacijskega sistema izberemo napačne parametre in se celoten računalniški sistem upočasni ali pa določena programska oprema, ki smo jo namestili, ne deluje. To lahko s pomočjo načina Keep odpravimo s preprostim ponovnim zagonom računalnika. Če s kartico delamo v administratorskem načinu, lahko poleg obeh že zgoraj omenjenih možnosti izberemo še varni način (*angl. save mode*), pri katerem se spremembe na sistemu shranijo v zaščiteni del trdega diska, medtem ko se dinamični del pomnilnika sprazni in je tako pripravljen na morebitne spremembe – nove podatke. Shranimo jih lahko čez prejšnjo ali zadnjo točko povratka ali pa naredimo novo točko povratka. Če imamo točk povratka več, lahko izbiramo, s katere naj se računalniški sistem postavi. Tako imamo lahko več točk povratka, ki ustrezajo različnim profilom uporabnikov, saj različni uporabniki potrebujejo za svoje delo različno programsko opremo. Šele ko kartica preide vse zgoraj opisane stopnje pri zagonu, se izvrši zagon operacijskega sistema. Delovanje kartice bi lahko ponazorili s spodnjim diagramom:



Slika 2: Diagram delovanja varnostne kartice Radix MLP [10].

2. 2. 1. Uporabniška izkušnja uporabe varnostne kartice

Šele ko razumemo delovanje in načine zagonov varnostnih kartic, se lahko lotimo inštalacije ali namestitve same strojne opreme (varnostne kartice) in njej pripadajoče programske opreme na javno dostopne računalnike. Najprej je treba na računalnike namestiti operacijski sistem in osnovno programsko opremo, kot so Office paket, predvajalniki videodatotek in podobno. Pred namestitvijo varnostne kartice je zelo pomembno pregledati trdi disk, da se prepričamo, da na njem ni zlonamerne programske kode (raznih oblik virusov, črvov, trojanskih konjev in podobno). To najlažje storimo s katerim od protivirusnih programov, ki ga namestimo na računalnik, preden začnemo z namestitvijo varnostne kartice. Prav tako je treba disk pregledati s programom, ki omogoča detekcijo ali zaznavo pokvarjenih datotek (*angl. corrupted files*). Če imamo na računalniku operacijski sistem Windows, lahko to storimo iz ukazne vrstice z ukazom chkdsk, ki mu sledi predpona particije, ki jo želimo pregledati.

Zaradi enostavnosti pri namestitvi kartice se na vseh računalnikih, na katere se namešča kartice, napravi le eno particijo diska. Zatem je treba disk, na katerem bo prostor za novonastale podatke, torej dinamični del pomnilnika, tudi defragmentirati – razdrobljene dele istega podatka

združiti skupaj ali jih umestiti blizu. Ta korak je zelo pomemben, saj se ob ustvarjanju novih točk povratka podatki slej kot prej razdrobijo, kar se pokaže v počasnejšem nalaganju posnetka.

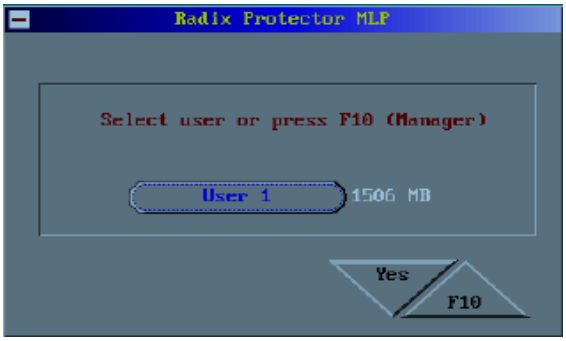
Preden pa se lahko lotimo namestitve kartice, je treba:

- začasno onemogočiti delovanje protivirusne programske opreme, saj bi lahko povzročila napako ob namestitvi kartice,
- onemogočiti morebitno protivirusno zaščito tudi v BIOS-nastavitvah,
- za prvo zagonsko napravo (*angl. primary boot device*) izbrati mrežno kartico (*angl. network card*),
- računalnik ugasniti in odklopiti z napajanja,
- odstraniti stranico računalnika in v prosto mesto na PCI-vodilu vstaviti kartico,
- odstranjeno stranico zopet priviti, priklopiti računalnik na napajanje in ga pognati.

Računalnik izvede svoj proces postavljanja (*angl. boot-up*) in nanj je treba namestiti še gonilnike za varnostno kartico. Ko računalnik naloži svoj operacijski sistem, v našem primeru Windows XP, lahko na spletni strani proizvajalca poiščemo gonilnike oziroma namestitveno datoteko. Zatem to datoteko poženemo in s tem sprožimo namestitveni postopek. Najprej je treba vpisati registracijsko številko, da se namestitveni postopek nadaljuje. Ko vtipkamo dvajsetmestno številko, se pojavi okence, ki ponuja tri možnosti za velikost dinamičnega dela pomnilnika, ki bo pripadal varnostni kartici. Izberemo lahko med možnostmi 100 MB, 200 MB, 500 MB ali 1 GB.

Slika 3: Izbira velikosti dinamičnega dela pomnilnika.

Ker smo imeli predvidenih kar nekaj naknadnih namestitev programske opreme, smo izbrali največjo možno kapaciteto – 1 GB. Izbira velikosti vpliva na to, koliko točk povratka lahko kasneje administrator ustvari. Nato se na računalniku sproži postopek namestitve oziroma inštalacije, ki »rezervira« del trdega diska in namesti že omenjene kazalce. Ko se namestitveni postopek zaključi, se pojavi okence uporabniškega vmesnika. Ko izbremo opcijo finish oziroma končaj, se računalnik ponovno zažene. Po začetnem POST (Power On Self Test) testu, ki preveri, če naprave, ki sestavljajo računalnik, delujejo, računalnik spet prikaže uporabniški vmesnik varnostne kartice, ki prikaže informacije o zaščitenem trdem disku. Med te informacije spada črka pogona oziroma trdega diska, v našem primeru, ko imamo samo eno particijo C:, pa velikost izbranega trdega diska in datotečni sistem (*angl. file system*) na nosilcu. Ko pritrdimo, kliknemo na gumb Yes in prikaže se naslednje sporočilo: Starting protector ... Po nekaj sekundah se pojavi glavno okno uporabniškega vmesnika, kjer lahko nastavimo parametre zaščite, ki jih potrebujemo za posamezni računalnik.



Slika 4: Glavno okno uporabniškega vmesnika varnostne kartice Radix MLP.

Prikaz tega menija hkrati pomeni, da se je varnostna kartica uspešno namestila. S pritiskom na tipko F10 se odpre konfiguracijski meni. Najprej je treba poskrbeti za administrativno geslo, saj lahko nove točke obnovitve sistema in naprednejše nastavitve upravlja le administrator. Iz glavnega menija izbremo opcijo Management. Za tem se pojavi novo okno, v katerem izbremo gumb Modify Maneger Password. S pritiskom na ta gumb se pojavi prazna vrstica, v katero vpišemo administratorsko geslo, saj je zaradi varnosti treba vnos ponoviti. Pri nekaterih verzijah kartic je treba v disketni pogon vstaviti še disketo, na katero se zapiše geslo, ki ga uporabimo, če geslo administrator pozabi. Ko je to opravljeno, pritisnemo na gumb Quit, s katerim se vrnemo v prvotno okno, na glavni nastavitveni meni.

Slika 5: Glavni nastavitveni meni varnostne kartice Radix MLP.

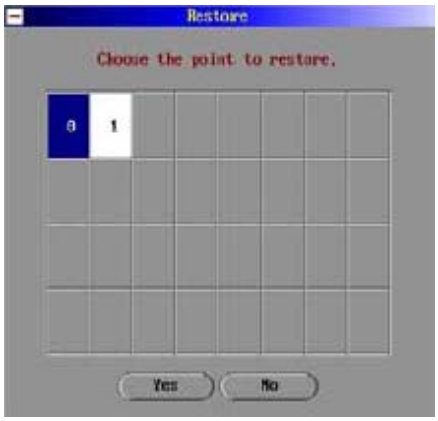
Naslednja stopnja je poimenovanje operacijskega sistema na zaščitenem nosilcu. To pride prav, če imamo računalnik z več operacijskimi sistemi (*angl. multi-boot*), hkrati pa nepooblaščenim uporabnikom prepreči dostop do operacijskega sistema. S pritiskom na gumb Modify User Password se nam prikaže vpisna vrstica, kamor napišemo ime operacijskega sistema na zaščitenem disku. Tudi tu je treba vnos ponoviti. Naslednji korak je poimenovanje uporabnikov računalnika. Ker je računalnik namenjen javni uporabi, pustimo prednastavljene

nastavitve. Vsi »navadni uporabniki« sistema imajo uporabniško ime USER 1. Nato spet pritisnemo na gumb Quit, s katerim se vrnemo v glavni konfiguracijski meni. Sledi nastavitev zagonske metode (*angl. boot method*) kartice. Tu lahko izbiramo med načini prikaza uporabniškega menija kartice ob zagonu in med nekaterimi drugimi možnostmi, kot je avtomatsko shranjevanje točk povratka. Za nastavitev teh možnosti v glavnem oknu ali meniju pritisnemo tipko F10, iz naslednjega okna izberemo opcijo Configuration, nato pa opcijo Boot methods. Pod opcijo Boot Methods se da izbrati med možnostmi Display menu, Scheduled Multi Point Save, Recover at Every Boot, Scheduled Restore in Keep Last Boot status. Če izberemo Display Menu, se grafični uporabniški vmesnik varnostne kartice prikaže med vsakim ponovnim zagonom računalnika, z izbiro Scheduled Multi Point Save pa lahko določimo, da se bo nova točka povratka avtomatično ustvarila v nekem časovnem obdobju – vsak dan, vsak drugi dan, vsak teden ali mesec. Sistem doda točko po novem zagonu, če je preteklo toliko časa, kot smo ga določili. Če izberemo, da se točka povratka ustvari vsak drugi dan, lahko po prvem dnevu ponovno poženemo računalnik in nova točka se še ne bo dodala. Ko bo računalnik prižgan še en dan, se bo za ponovnim zagonom avtomatično ustvarila točka povratka. Z izbiro opcije Recover at Every Boot se sistem vedno, torej ob vsakem ponovnem zagonu, avtomatično vrne na povratno točko nič (*angl. point 0*). To je tudi možnost, ki jo izbremo, saj se ob vsakem novem zagonu sistem postavi iz želene točke. Ta možnost je priporočena za javne računalnike. Možnost Scheduled Restore omogoča vrnitev sistema na točko nič ali Point 0 ob fiksnih časovnih intervalih (po enem ali dveh dnevih, po enem tednu ali po enem mesecu). Možnost Keep Last Boot Status pa zagotavlja stanje sistema kot pred ponovnim zagonom. Ko zaključimo z nastavitvami in namestitvijo varnostne kartice, jo še preizkusimo. To storimo tako, da na namizje operacijskega sistema posnamemo tekstovno datoteko in ponovno zaženemo računalnik. Ker je tudi preprosta tekstovna datoteka sprememba trdega diska, lahko zaključimo, da je kartica pravilno nameščena in deluje, če se po ponovnem zagonu omenjena tekstovna datoteka ne prikaže. S tem je namestitev kartice zaključena.

Večkrat pa se zgodi, da moramo določeno programsko opremo namestiti po opravljeni inštalaciji varnostne kartice. Takrat je pred zagonom operacijskega sistema, ko se na zaslonu prikaže sporočilo Starting Radix Protector, treba najprej pritisniti kombinacijo tipk Alt + F10, s katero pridemo do glavnega menija kartice. Opisana kombinacija je potrebna zato, ker je kartica v načinu Recover at Every Boot, v katerem se uporabniški vmesnik ne prikaže samodejno. Nato s s pritiskom gumba F10 izberemo administratorski način (*angl. maneger mode*) upravljanja računalnika, saj je spremembe oziroma novo namestitev programske opreme možno shraniti le v tem načinu. Ko vtipkamo administratorsko geslo, imamo v zavihku Boot Options na izbiro štiri načine, v katerih se lahko sistem zažene. To so Keep Data, Add Point, Save Data in Restore Data. Prva možnost po ponovnem zagonu ohrani status zadnjega zagona, zato je idealna za preizkus uspešnosti namestitve novih apliakcij oziroma nove programske opreme. Možnost Add Point omogoča ročno ustvarjanje nove točke povratka.

Slika 6: Dodajanje nove točke obnovitve.

Kot zanimivost naj omenim, da je edina omejitev pri dodajanju novih točk povratka prostor na zaščitenem trdem disku, medtem ko so starejši modeli kartic omogočali tri do šest novih točk povratka. Možnost Save Data shrani vse spremembe na sistemu. Slaba stran te možnosti je, da vedno shrani stanje kot točko nič ali Point 0. Tako lahko neizkušen uporabnik na začetku izbere možnost Keep Data, naredi spremembe na sistemu, ob ponovnem zagonu pa jih shrani. Tu se pojavi tveganje, da uporabnik ob napaki pri namestitvi presname točko nič s posnetkom nedelujočega sistema ali nedelujočo novo nameščeno programsko opremo. Zato je treba vedno, kadar se dodaja nova programska oprema, najprej izbrati možnost Keep Data, nato pa v naslednjem koraku (še pred nameščanjem) dodati točko povratka, ki je kopija prejšnje in ima le drugo ime. To storimo z izbiro možnosti Add Point. Ko izberemo to možnost, se na zaslonu pokaže vnosna vrstica, v katero zapišemo ime »nove« točke povratka. Najbolje je, da izberemo ime, ki bo opisovalo namen nastanka nove točke povratka. Kartica datum in čas nastanka nove točke doda samodejno in tako administratorju olajša delo, ko le-ta določa točko, iz katere se bo sistem pognal. Ko napravimo varnostno kopijo sistema, se lahko lotimo namestitve nove programske opreme in ponovno poženemo računalnik. Na tem mestu spet sledi kombinacija tipk Alt + F10, s katero na zaslon prikličemo uporabniški vmesnik kartice. Preostane le še, da prijavljeni adiminstrator sistema shrani podatke. Spremembe so se shranile v točko nič, medtem ko je bila kot točka ena shranjena kot stanje sistema pred novim nameščanjem programske opreme. Nato se v glavnem meniju izbere gumb User in nato še gumb Restore Options. Po pritisku le-tega se na zaslonu prikaže razpredelnica, v kateri so zapisane točke povratka, kot točka nič, ena in tako naprej. S klikom na katerokoli točko se v meniju prikaže ime, čas in datum nastanka povratne točke. S klikom na točko povratka jo označimo kot aktivno, torej kot točko, s katere naj se sistem postavi. V našem primeru je bila to točka ena.



Slika 7: Izbiranje točke zagona.

Enak postopek lahko uporabimo, ko je treba shraniti posodobitve operacijskega sistema ali protivirusne zaščite. Na tem mestu naj opozorim samo na to, da z dodajanjem novih točk povratka znatno upočasnimo zagonski proces računalnika [9, 10].

V naslednjem poglavju bom opisal delo z najbolj razširjenimi različicami programske opreme, ki je namenjena obnavljanju in zaščiti javnih računalniških sistemov [9, 10].

2. 3. Programska oprema, namenjena preprečevanju izpada računalniškega sistema

V tem poglavju bom opisal delo z najbolj razširjenimi različicami programske opreme, ki služi obnavljanju in zaščiti javnih računalniških sistemov.

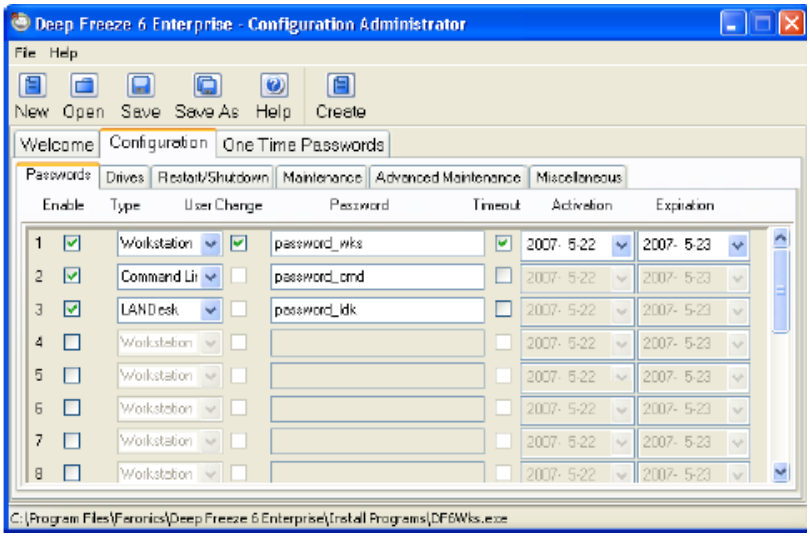
2. 3. 1. Deep Freeze

Med raziskovanjem programske opreme, ki je namenjena obnovi in varovanju računalniškega sistema, sem najprej naletel na zelo razširjeno rešitev, program Deep Freeze. Tudi ta program temelji na tehnologiji naloži in obnovi. Le-ta, kot že rečeno, stanje računalniškega sistema postavi v stanje, kakršno je bilo ob namestitvi programa, hkrati pa administratorju omogoča delo na daljavo. Ob namestitvi te programske opreme je treba na trdem disku, kamor jo posnamemo, zagotoviti vsaj 1 GB prostora. Glede na ta podatek lahko sklepamo, da je delovanje tega programskega orodja podobno delovanju varnostnih kartic, saj se tudi pri programu Deep Freeze ne ustvari fizična slika, ampak je povratek sistema zagotovljen s kazalci na »nove« datoteke in na tiste, ki so ob namestitvi programa Deep Freeze že bile prisotne. Enako kot varnostne kartice tudi ta programska oprema obravnava že eno samo tekstovno datoteko, ki jo ustvari uporabnik, za spremembo na trdem disku. Omenjeno programsko opremo sem izbral predvsem zato, ker administratorjem omogoča namestitev in delo na daljavo, hkrati pa lahko iz enega centralnega računalnika upravljamo z vsemi drugimi delovnimi postajami, na katerih je nameščena ta programska oprema, kar pri varnostnih karticah oziroma vsaj pri modelih, s katerimi sem imel opravka, ne drži. Opisal bom postopek namestitve, uporabe in vzdrževanja programske opreme Deep Freeze.

Najprej si je treba zamisliti, kako naj bi izgledala topologija varnostnega sistema. Ker je programska oprema namenjena javnim računalnikom, torej računalnikom v šolah, knjižnicah in ostalih izobraževalnih ustanovah, se lahko odločimo za naslednjo postavitev računalnikov. Na usmerjevalnik priključimo tri delujoče računalnike, od katerih je eden strežnik (v realnem okolju bi to bil učiteljev ali knjižničarjev računalnik), druga dva pa sta javna računalnika. Na vse tri računalnike namestimo kopijo operacijskega sistema Windows XP. Najprej zagotovimo, da so vsi trije računalniki dobili svoj IP preko DHCP-strežnika oziroma usmerjevalnika. Ker delujemo v LAN-omrežju, so lahko ti trije IP-naslovi dinamični. To storimo tako, da v Nadzorni plošči operacijskega sistema Windows izberemo ikono Omrežne povezave, kliknemo desno na ikono Local Area Connection in v meniju izbremo možnost Properties. V naslednjem oknu izbremo možnost Internet Protocol (TCP/IP) in možnost Properties. V novoprikazanem oknu izberemo možnost Obtain an IP address automaticlly in možnost Obtain DNS server automaticlly. Sledi potrditev izbranega s pritiskom na gumb Ok. Nato preverimo povezavo s spletom in se lotimo namestitve same programske opreme Deep Freeze. Izbral sem različico Deep Freeze Enterprise, ki podpira delo in upravljanje delovnih postaj na daljavo. Deep Freeze Enterprise vsebuje pet programskih modulov oziroma komponent. Deep Freeze Configuration Administrator installation file ali nastavitvena datoteka je namenjena namestitvi na centralnem računalniku oziroma Deep Freeze strežniku. Ob namestitvi te datoteke se na centralnem računalniku ustvarita dve komponenti. Prva, Deep Freeze Configuration Administrator, je namenjena ustvarjanju inštalacijskih datotek za delovne postaje. Druga, Deep Freeze Enterprise Console, je namenjena spremljanju stanja delovnih postaj ter izvršitvi ukazov in nalog za delovne postaje. Preostali dve komponenti, Deep Freeze workstation installation file in Deep Freeze workstation Seed, sta namenjeni javnim računalnikom.

Slika 8: Moduli programske opreme Deep Freeze.

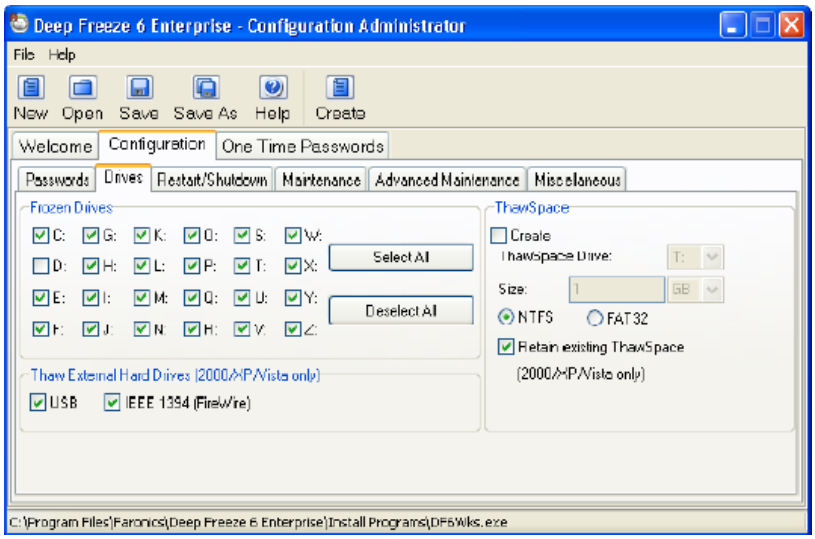
S spleta prenesemo na centralni računalnik datoteko Deep Freeze Configuration Administrator installation file in jo poženemo. S pritiskom na gumb Install se na računalnik namestita komponenti Deep Freeze Configuration Administrator in Deep Freeze Enterprise Console. Nato se lahko lotimo ustvarjanja namestitvene datoteke za javne računalnike s pomočjo programske komponente Deep Freeze Configuration Administrator. Ob dvokliku na to datoteko se pojavi okno, v katerem lahko izberemo možnosti za ustvarjanje inštalacijske datoteke, ki jo kasneje namestimo na javne računalnike. V oknu Deep Freeze Configuration Administrator imamo na voljo tri zavihke. Prvi med njimi je zavihek Welcome, v katerem so podatki o uporabniku in naslov spletne strani podjetja, ki je programsko opremo izdelalo. Naslednji zavihek Configuration ponuja možnosti nastavitve inštalacijske datoteke, s katero se program namesti na javne računalnike. Pod zavihkom Configuration se nahaja še šest novih zavihkov. V prvem – Passwords – nastavimo geslo za dostop do menija programa Deep Freeze na ciljnih oziroma javnih računalnikih, lahko pa izberemo tudi čas, ko se bo geslo izteklo. V tem primeru je treba geslo po izteku ponovno nastaviti. Ta opcija zagotavlja dodatno varnost.



Slika 9: Zavihek Passwords.

V naslednjem zavihku Drives so črke particij diska od C: do Z:. Z označitvijo particij določimo, katere particije hočemo zavarovati, zaščitene particije pa se imenujejo Frozen Drives. Razlog, da nam program ponuja particije kar od C: do Z:, je v tem, da lahko eno inštalacijsko datoteko namestimo na več računalnikov, ki strojno niso nujno enaki. V primeru, da ciljni računalnik nima particije diska, ki jo označimo kot zavarovano, se ne zgodi nič. Tako so varovane samo particije, ki na ciljnih računalnikih dejansko obstajajo. Pod črkami particij obstaja možnost, da zamrznemo tudi zunanje pomnilne naprave (npr. zunanji disk, ki ga priključimo na

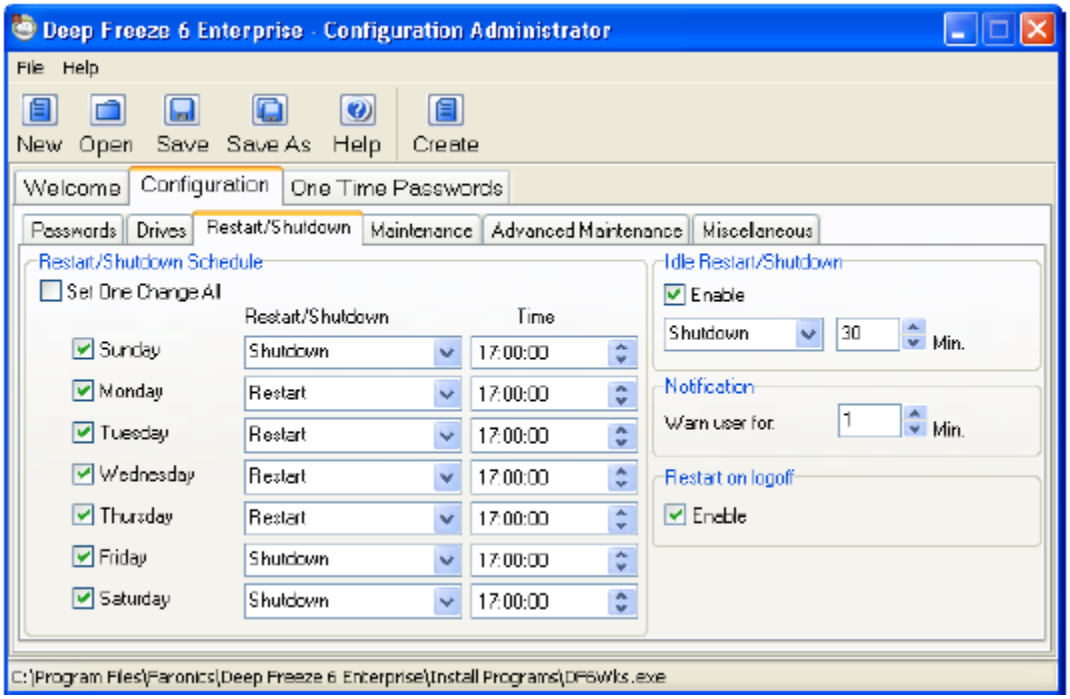
USB-vhod). Kljub temu da pustimo zunanje naprave v »normalnem« stanju, se lahko zgodi, da računalnik pripne zunanjo pomnilno napravo pod črko, ki je označena v meniju. V tem primeru bodo zunanje naprave zaščitene – ustvari se posnetek naprave, in ko jo nehamo uporabljati, se le-ta povrne v stanje pred uporabo. To je lahko zelo nerodno, saj se zunanje naprave ponavadi uporabljajo za prenos podatkov, v tem primeru pa novo posnetih podatkov na zunanji pomnilni napravi ni. Zatem se ustvari navidezno particijo pomnilne naprave, na katero se bo namestil program Deep Freeze. To naredimo tako, da v zavihku Drives označimo gumb Create Thaw Space. Ta navidezna particija, ki se ustvari na trdem disku, na katerega se namesti program Deep Freeze, je namenjena temu, da se nanjo lahko prenesejo podatki, ki tam ostanejo tudi po ponovnem zagonu računalnika. Configure Administrator ponuja možnost izbire črke navidezne particije, ki jo bo pripel operacijski sistem. Ker smo na testnih računalnikih napravili samo eno particijo diska, ki se v okolju Windows tipično pripne kot C:, smo za navidezno napravo izbrali črko D:. Program nam ponudi možnost določitve velikosti te navidezne particije. Najmanjša možnost je 16 MB, največja pa kar 1 TB. Ker smo imeli na testnih računalnikih disk velikosti 40 GB, smo se odločili, da za navidezno particijo porabimo 10 GB. Naslednji korak je določitev datotečnega sistema v navidezni particiji. Ker operacijski sistem Windows XP tipično uporablja NTFS datotečni sistem, se odločimo zanj. S potrdivijo s pritiskom na gumb Retain Existing Thaw Space lahko določimo, da se virtualna particija zadrži na trdem disku tudi po morebitni deinštalaciji programa Deep Freeze. Ta možnost je dobrodošla, saj se ta del trdega diska uporablja za podatke, ki jih želimo obdržati in so za uporabnike pomembni. Poleg tega je Thaw Space dobrodošel tudi zato, da na delu diska ali particiji, kjer je Deep Freeze, ne smemo imeti nameščenih nobenih antivirusnih programov, saj s tem tvegamo nezanesljivo delovanje našega programa. To lahko preprosto rešimo s tem, da z nameščanjem protivirusne programske opreme počakamo do končane namestitve programa Deep Freeze, in jo zatem posnamemo na particijo Thaw Space.



Slika 10: Zavihek Drives.

Naslednji zavihek v Configure Administrator-ju se imenuje Restart/Shutdown. Vsebuje imena dnevov v tednu in s pritiskom na gumb pred imenom izbranega dne le-tega označimo kot aktivnega. Zatem lahko iz menija izberemo opcijo Restart ali Shutdown, ponovno poženi ali ugasni računalnik. Tako lahko določimo, katera akcija se bo izvršila na delovnih postajah ob

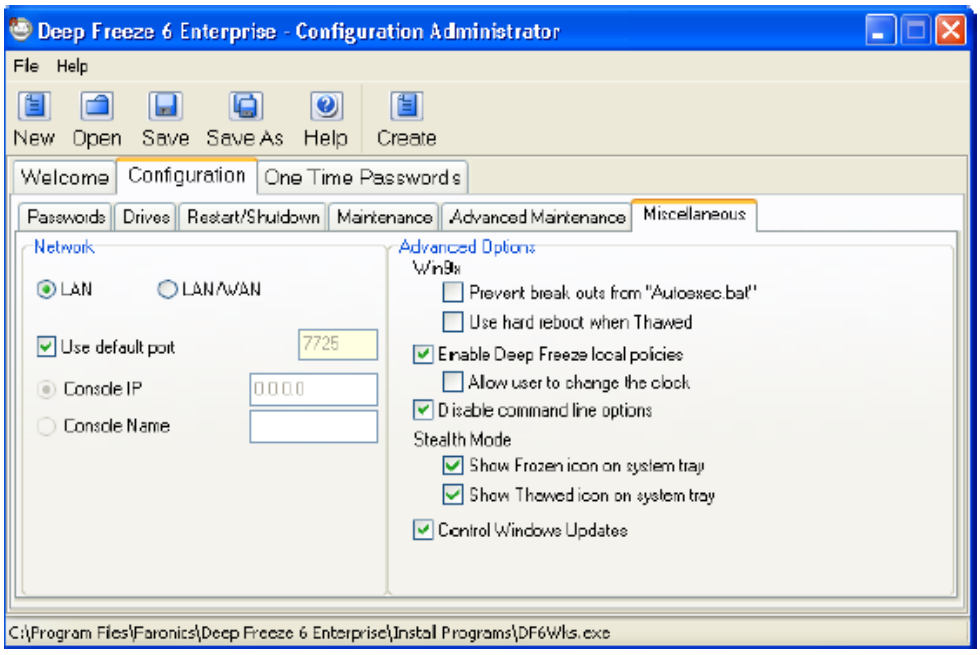
katerem dnevu. Poleg dneva v tednu in vrste akcije, ki se lahko izvrši, lahko iz menija Time izberemo tudi uro, ob kateri se želena akcija lahko izvrši. V zavihku Restart/Shutdown se nahaja tudi opcija, s katero lahko določimo, da se računalnik ponovno požene ali ugasne, če je nekaj časa neaktiven (*angl. idle*). Kot neaktivni čas se »šteje« čas, v katerem uporabnik ne pritisne na nobeno tipko na tipkovnici ali miški, razen za celozaslonske (*angl. full screen*) programe. Če je čas neaktivnosti uporabnika pretečen, lahko določimo tudi, kako dolgo bo na ekranu sporočilo, ki uporabnike obvešča, da se bo računalnik ponovno zagnal ali ugasnil. V naslednjem zavihku Configure Administrator-ja Maintenance imamo možnost izbire, ob katerih dnevih v tednu in ob katerih urah se bo posodobil operacijski sistem, in možnost, da se računalnik po posodabljanju samodejno ugasne. Z izbiro določenega časa posodabljanja ne zagotovimo, vendar sistemu damo čas, v katerem lahko izvede posodobitve, ki se bodo na njem poznale. Tukaj lahko med postopkom posodabljanja uporabnikom tudi onemogočimo uporabo miške in tipkovnice z označitvijo gumba Disable Keys. Kot že rečeno, lahko nastavimo dan in uro pričetka in konca posodabljanja, pri čemer pa je treba paziti, da izberemo čas, v katerem bo računalnik prižgan. Če na primer nastavimo v zavihku Restart/Shutdown neko uro v dnevu tedna, ob kateri se računalnik ugasne, se v tem času operacijski sistem ne more posodobiti.



Slika 11: Zavihek Restart/Shutdown.

Naslednji zavihek Advanced Maintenance je namenjen določitvi SUS (Microsoft Software Update Service) in/ali WSUS (Windows Software Update Service) strežnikov, ki so, kot že ime samo pove, namenjeni za hranjenje in prenos posodobitev operacijskega sistema Windows oziroma Windows programske opreme. Vse kar je treba storiti, je vpis IP-strežnika. Tega nismo storili, saj dobi v primeru, ko ne vpišemo IP-naslova strežnika oziroma obeh strežnikov, delovna postaja posodobitve preko interneta. Prednost WSUS oziroma SUS-strežnika pa je le ta, da vse delovne postaje dobijo hkrati enake posodobitve, medtem ko v primeru, če strežnika ali eden izmed njiju nista označena, delovne postaje dobijo posodobitve posamično.

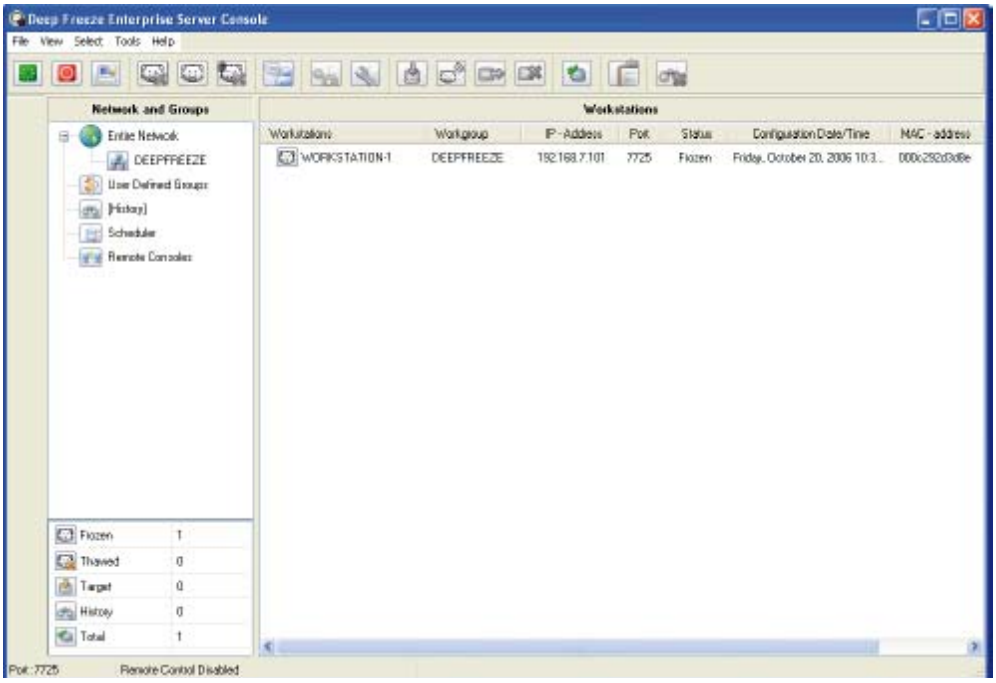
Naslednji zavihek je med najpomembnejšimi, saj z njim določimo omrežne nastavitve. Program Deep Freeze podpira dve vrsti mrežnih komunikacij. Prva je med računalnikom, na katerem je nastavljen Deep Freeze Console, in delovno postajo, druga pa med dvema računalnikoma z inštalacijo Deep Freeze Console. V zavihku Miscellaneous tako lahko izberemo način povezave med delovno postajo in Deep Freeze strežnikom z nameščenim Deep Freeze Console modulom. Na izbiro sta dva tipa povezav: LAN in LAN/WAN. Ker smo imeli vse tri računalnike priključene na en usmerjevalnik, to je na enem podomrežju, smo izbrali opcijo LAN. LAN-povezava zahteva samo še določitev vrat (*angl. port*). Program Deep Freeze ima rezervirana vrata 7725. Izbira pravih vrat je zelo pomembna – če vrata niso dosegljiva, ker jih uporablja že neka druga programska oprema, ne bomo dosegli povezanosti strežnika in delovnih postaj. Oba računalnika (delovna postaja in strežnik z nameščenim modulom Deep Freeze Console) se namreč med seboj »najdeta« prek UDP-broadcastov, ki se izvajajo samo takrat, ko se požene ali delovna postaja ali strežnik. S tem se zagotavlja najmanjša možna obremenitev mrežnih povezav. Če izberemo možnost LAN/WAN, je treba poleg številke vrat določiti še IP-številko strežnika ali ime strežniškega računalnika. Če izberemo IP-možnost, je treba na strežniku nastaviti statičen IP, če pa vpišemo ime strežniškega računalnika, je ta IP lahko dinamičen, torej spremenljiv. Ta možnost je izredno dobrodošla v primeru, ko administrator sistema ne mora biti na mestu, kjer je strežniški računalnik. Tako lahko na primer na domači računalnik namesti Deep Freeze Console in se prek tega računalnika poveže s strežniškim računalnikom, prek te povezave pa dobi dostop do delovnih postaj. Ta možnost povezave se zato imenuje Console to Console.



Slika 12: Zavihek Miscellaneous.

Ko zaključimo z nastavljanjem vseh zgoraj opisanih možnosti, ustvarimo namestitveno datoteko za delovne postaje. To storimo s pritiskom na gumb Create v Configure Administratorju. Na tem mestu lahko izbiramo med ustvarjanjem dveh datotek. Prva se imenuje

Deep Freeze Workstation Seed in vsebuje samo mrežne nastavitve, ki omogočajo, da je delovna postaja vidna v okolju Console. Druga možnost je ustvariti Deep Freeze Workstation Installation File, ki namesti verzijo programa Deep Freeze na delovno postajo z vsemi možnostmi, ki jih izberemo v okolju Configure Administrator. Ustvarimo obe datoteki in ju shranimo. Zatem namestimo Deep Freeze Workstation Seed na oba testna oziroma »javna« računalnika. Tu je treba le dvoklikniti na ikono Deep Freeze Workstation Seed. Med nastavitvijo ni treba storiti nič drugega, kot pustiti računalnik, da z njo konča, saj se vmes ne ponujajo nobene druge možnosti. Ko se namestitev zaključi, se delovna postaja ponovno zažene. Nato je treba preveriti, če je delovna postaja vidna v okolju Console. Ker so računalniki priključeni na usmerjevalnik, je treba na njem odpreti vrata, ki jih program uporablja. S tem zagotovimo, da usmerjevalnik spusti naprej promet, ki je povezan s programom Deep Freeze. Kljub temu v okolju Console delovna postaja še ni bila vidna. Kar nekaj časa smo potrebovali, da smo ugotovili, da sta na obeh računalnikih aktivirana požarna zidova Windows. Zato je bilo treba v operacijskem sistemu Windows na obeh računalnikih odpreti kontrolno ploščo in izbrati ikono Windows Firewall. V oknu, ki se odpre, izberemo zavihek Exceptions. Iz menija v zavihku Exceptions izberemo Add program in iz ponujenega menija programske opreme, ki je nameščena na računalnik, program Deep Freeze. Sledi še nastavitev vrat, ki jih ta program uporablja. To storimo tako, da v zavihku Exceptions izberemo gumb Add port. Ob pritisku na ta gumb se najprej poimenuje program, torej Deep Freeze, vpiše številko vrat, ki jo program uporablja, nato pa še označi UDP-protokol, saj se prek tega protokola »vidita« strežnik in delovna postaja. Zatem se požene modul Console. Tako je bila delovna postaja vidna. Deep Freeze administratorjem ponuja možnost Target Install, kar pomeni, da lahko administrator namesti Deep Freeze Workstation Installation File, dejansko verzijo Deep Freeze programa, na oddaljeno delovno postajo. Workstation Seed je torej namenjen le temu, da se oba računalnika lahko povežeta, ne namesti pa dejanske verzije programa. Workstation Seed se namesti izredno enostavno, saj je potreben le dvoklik na ikono. Tako lahko to namestitev opravi kdorkoli in ne zahteva administratorjeve fizične prisotnosti. V okolju Console nato izberemo oba računalnika in pritisnemo na možnost Target Install. Okolje Console zatem zahteva Deep Freeze Workstation Installation File, ki smo ga prav tako ustvarili po postopku, opisanem v začetku poglavja. Nato določimo še mesto, kjer se nahaja že pripravljena namestitvena datoteka. Sprožimo namestitveni postopek. Ko se namestitev zaključi, preskusimo namestitev programske opreme z že opisanim postopkom. Na delovni postaji ustvarimo tekstovno datoteko, jo posnamemo na namizje in ponovno zaženemo računalnik. Tekstovne datoteke po ponovnem zagonu delovne postaje ni bilo več na namizju. Ker pa se program Deep Freeze požene znotraj operacijskega sistema, ne ščiti zagonskega procesa računalnika, kot ga varnostne kartice. Tako je treba v BIOS nastavitvah nastaviti trdi disk kot prvo napravo, s katere zaženemo operacijski sistem, in zaščititi dostop do BIOS-a z geslom. Tako preprečimo zagon sistema iz prenosljivega pomnilnega medija (diskete, CD-ROM-a ali zunanjega diska) in s tem dobimo dodatno stopnjo varnosti. Tako je namestitev zaključena.



Slika 13: Pogled na delovne postaje iz okolja Console.

Vse nadaljnje operacije (posodobitve programa Deep Freeze, zaklenitev tipkovnice in miške na delovnih postajah, pošiljanje sporočil delovnim postajam, deinštalacija programa Deep Freeze, ponovni zagon v »zamrznjenem« in »odtajanem« stanju, ponovni zagon ali izklop delovnih postaj) je mogoče opravljati iz oddaljenega strežniškega računalnika [4].

2. 3. 2. Symantec Norton Ghost

Med delom s programsko opremo Deep Freeze sem večkrat zasledil, da se kot največja »konkurenca« programu Deep Freeze omenja Norton Ghost. Programa sta primerljiva v smislu, da sta oba sposobna narediti posnetek pomnilne naprave, prav tako pa sta sposobna ta posnetek kasneje tudi obnoviti na pomnilni napravi. Programska oprema Norton Ghost je pravzaprav programska oprema, ki nam omogoča kloniranje trdega diska. To pomeni, da Norton Ghost »naredi« posnetek trdega diska in vsebino spravi v datoteko s tipično končnico .v2i, ki pomeni Norton Ghost Virtual Volume Image. Posnetek trdega diska se spravi v datoteko, ki predstavlja virtualno pomnilno napravo. Ta posnetek trdega diska lahko v okolju Ghost pripnemo kot pomnilno napravo in raziščemo njeno vsebino ali pa posnetek diska pripnemo na dejansko pomnilno napravo. Program Norton Ghost ne napravi bitne slike trdega diska, celotna vsebina diska se torej ne zapiše v sliko. V sliko se zapiše le toliko podatkov, kolikor jih je fizično prisotnih na disku, prazne bloke diska pa program Norton Ghost izpusti. S tem Norton Ghost doseže, da so slike relativno majhne, kar pomeni, da se lahko na majhen prostor shrani več posnetkov neke pomnilne naprave.

Norton Ghost omogoča tudi shranjevanje slik na oddaljeni lokaciji in obnavljanje oziroma pripenjanje slike trdega diska iz oddaljene lokacije, zaradi česar je ta programska oprema še posebej uporabna. V primeru okvare računalnika lahko preprosto preko uporabniškega vmesnika programa Norton Ghost sliko diska posnamemo na želeno napravo. Če je računalnik okvarjen do

te mere, da se operacijski sistem noče zagnati, lahko sliko diska prenesemo na trdi disk s pomočjo pogonskega CD-ja, ki ga ustvarimo s programom Norton Ghost.

Kot pri preizkusu programske opreme Deep Freeze poskušamo simulirati okolje, kakršnega bi lahko srečali v knjižnicah ali v šolah. Na usmerjevalnik, ki je služil tudi kot DHCP-strežnik, priključimo tri računalnike. Od teh sta bila v našem primeru dva enaka, kar pomeni, da sta računalnika enega proizvajalca z isto strojno opremo predstavljala javno dostopne računalnike, eden pa je predstavljal strežnik, na katerega shranjujemo tako imenovane točke povratka oziroma slike. Najprej na vse tri računalnike namestimo operacijski sistem Windows XP, saj je Norton Ghost ustvarjen oziroma združljiv z operacijskim sistemom Windows. Na obeh javnih računalnikih nastavimo dinamičen IP, na strežniku pa nastavimo statičen IP. To storimo tako, da v oknu Kontrolna plošča izbremo možnost Omrežne povezave. Z desnim klikom na LAN-ikono se pojavi meni, v katerem izberemo Možnosti. V novem oknu izberemo opcijo Internet Protocol TCP/IP. Nato pritisnemo na gumb Properties. V novem oknu določimo možnost Use the following Ip address. Ker je bil router nastavljen tako, da lahko dinamični IP nastavi petdesetim odjemalcem, s pričetkom na naslovu 192.168.1.100, se za IP-naslov izbere številko 192.168.1.11, ki je izven obsega dinamičnih naslovov. Ko vpišemo ta naslov, se v naslednjem polju Subnet mask samodejno izpiše številka maske, v našem primeru 255.255.255.0. Nato se za privzeti prehod (*angl. default gateway*) in primarni DNS-strežnik nastavi kar IP naslov usmerjevalnika, številka 192.168.1.1. Tako je bil strežnik nastavljen na statični IP, kar pomeni stalno dosegljivost na tej številki. Na obeh javnih računalnikih, ki sta imela samo 40 GB trdega diska, smo pustili le eno particijo, na strežniku pa smo imeli 160 GB trdega diska in smo zato lahko ob namestitvi ustvarili dve particiji. Prva particija C: je bila velikosti 20 GB, nanjo smo namestili operacijski sistem. Druga particija D:, ki je predstavljala odložišče za slike, pa je bila velika 140 GB. Na oba testna računalnika smo namestili še osnovno uporabniško programsko opremo. Zaradi kasnejših operacij je zelo pomembno, da se pri namestitvi operacijskega sistema na obeh javnih računalnikih ustvari administratorsko geslo. Na en javni računalnik smo namestili programsko opremo Norton Ghost. Ob namestitvi programa se je izvedel postopek, ki preveri gonilnike, nameščene na računalniku, in jih primerja z gonilniki na Norton Ghost namestitvenem CD-ju. Če program ugotovi, da kateri izmed gonilnikov, ki jih uporablja računalnik, ni na voljo na namestitvenem CD-ju, izpiše sporočilo z imenom manjkajočih gonilnikov. Ti so zelo pomembni, saj lahko le z zagotovitvijo ustreznih gonilnikov uporabljamo pogonski CD, ki ga ustvarimo s programom Ghost. Gonilniki namreč skrbijo za komunikacijo s strojnimi komponentami, kot so mrežna kartica, trdi disk ter tudi računalniška miška. Če nam katerikoli od gonilnikov manjka, v tako imenovanem Recovery okolju, ki ga poženemo preko pogonskega CD-ja, ne moremo dostopati do diskov, strežnika, na katerem imamo spravljene slike, ali imamo težave s katerokoli strojno napravo, ki sestavlja računalnik.

Slika 14: Glavno namestitveno okno programa Norton Ghost.

Namestitev začnemo tako, da v CD-ROM enoto računalnika vstavimo CD s programom Norton Ghost. Na zaslonu se pojavi uporabniški vmesnik, preko katerega najprej izberemo možnost Run Driver Validation. S tem se zažene zgoraj opisani postopek, ki primerja gonilnike. Med tem postopkom je program Norton Ghost naletel na nekaj gonilnikov, ki niso vključeni na namestitvenem CD-ju. V tem primeru program Norton Ghost ponuja možnost, da lahko uporabnik sam ustvari pogonski CD, s katerim zažene okolje Recovery. Pred tem je treba izvesti namestitev programske opreme Norton Ghost. To storimo tako, da v uporabniškem vmesniku namestitvenega CD-ja izberemo opcijo Install Norton Ghost. Ko se namestitev zaključi, se program samodejno zažene in ob prvem zagonu preveri posodobitve novejše različice. Ko je ta postopek zaključen, lahko dostopamo do uporabniškega vmesnika programa Norton Ghost. Najprej se lotimo postopka ustvarjanja pogonskega CD-ja. To storimo tako, da v uporabniškem vmesniku okolja Norton Ghost pritisnemo na gumb Tasks in izberemo opcijo Create Recovery Disk. Norton Ghost pri tem postopku zahteva, da vstavimo originalni namestitveni CD programske opreme in pritisnemo gumb Next. Nato v CD enoto vstavimo prazen CD, na katerega se zapiše vsebina pogonskega CD-ja. Program nam ponuja dve možnosti. Lahko izberemo način Automatic, kjer pustimo programu, da sam poišče ustrezne gonilnike in jih vključi na Recovery CD, lahko pa izberemo način Custom in sami poiščemo gonilnike za ustrezne strojne komponente računalnika. Izbrali smo opcijo Automatic in po približno desetih minutah smo imeli tako imenovan Custom Recovery Disk.

Uporaba programa Norton Ghost je sestavljena iz treh najpomembnejših potopkov:

Najprej moramo definirati oziroma določiti vrsto varnostne kopije (*angl. backup*). Pri tem se je potrebno vprašati:

- kaj,
- kdaj,
- kam.

Pri vprašanju kaj nas zanima, sliko katerega trdega diska želimo ustvariti. Ker smo imeli na obeh testnih računalnikih samo en fizični disk C:, smo ga določili kot tistega, katerega slika se bo ustvarila. Nadalje nas zanima, kdaj naj se ustvari slika trdega diska. Program Norton Ghost namreč ponuja možnost, da najprej naredimo celotno sliko trdega diska, imenovano Recovery Point. Ko imamo prvo sliko trdega diska varno spravljeno na določenem mestu, lahko periodično dodajamo inkrementalne slike, v katerih je zapisana samo sprememba stanja trdega diska od zadnje celotne varnostne kopije trdega diska. Tretje vprašanje kam se nanaša na lokacijo, kamor se slika določenega trdega diska spravi.

Drugi postopek pri uporabi Norton Ghosta je samo izvajanje nastajanja varnostne kopije oziroma pisanje v sliko. Tu je treba določiti, ali se bo postopek pisanja sprožil ročno po določenem urniku ali pa pri zaznavi določenih dogodkov na računalniku. Program Norton Ghost lahko nastavimo tako, da se slika trdega diska ustvari vedno, ko na računalnik nameščamo kakšno novo programsko opremo. Večkrat se namreč zgodi, da nam ob nepravilni inštalaciji določene programske opreme računalnik odpove, ali pa se zmanjša njegova hitrost procesiranja podatkov, kar uporabnik vidi kot upočasnitev sistema.

Tretji postopek se nanaša na obnovitev računalniškega trdega diska. Gre za zamisel, da se na strežniški računalnik prenaša slike trdega diska, ki jih lahko uporabimo za obnovitev sistema. Ker program Norton Ghost vsebuje vgrajeni FTP-odjemalec, smo si zamislili, da na strežniški računalnik namestimo FTP-strežnik, s katerim bi lahko prenašali sliko od testnega računalnika na strežnik. Program Norton Ghost namreč omogoča možnost Offsite Copy, s katero lahko prenesemo sliko delujočega trdega diska na strežnik. Poleg FTP-načina omogoča tudi pošiljanje slike trdega diska v deljene mape (*angl. shared folders*). Zato je bilo najprej treba poskrbeti za pravilne nastavitve na strežniku.

Najprej na strežniškem računalniku, na particiji D:, ustvarimo mapo, poimenovano Backup, ki jo uporabljamo za odložišče slik. To storimo tako, da kot običajno ustvarimo novo mapo, zatem pa v oknu Local disk D: izberemo možnost Tools in Folder Options. Nato v oknu Folder Options kliknemo na zavihek View in odznačimo možnost Use simple file sharing. To storimo zato, da kasneje lahko označimo pravice uporabnikov pri dostopu in spreminjanju datotek v deljeni mapi. Nato z desno miškino tipko kliknemo na mapo Backup in izberemo možnost Sharing and security. V oknu, ki se pojavi, izberemo možnost Sharing in označimo gumb Share this folder. Nato v istem oknu pritisnemo na gumb Permissions in kliknemo na gumb Add. Zatem dodamo uporabnika, ki je določen kot administrator računalnika, ki smo ga ustvarili že ob namestitvi operacijskega sistema, in mu dodelili pravice za popolno kontrolo spreminjanja in dodajanja datotek v mapi Backups. Nato je treba poskrbeti še za FTP-strežnik na strežniškem računalniku. To lahko storimo tako, da na računalnik namestimo FTP-server FileZilla.

Ker smo imeli vse tri računalnike na LAN-omrežju, priključene na usmerjevalnik s storitvijo NAT, je bila nastavitev relativno enostavna, saj ni bilo treba določati zunanjih in notranji vrat, kot bi bilo potrebno v primeru, če bi imeli strežnik na drugem podomrežju kot testna računalnika. Na usmerjevalniku je bilo treba označiti le vrata, preko katerih se je prenašal promet, povezan s programom Norton Ghost. Ker pa je za FTP-prenose značilno, da se povezava med računalnikoma ustvari preko enih vrat, sami podatki pa se prenašajo med drugimi vrati, smo za podatkovna vrata pustili kar prednastavljeno številko 21. Tudi tu je bilo treba, podobno kot pri programu Deep Freeze, na vseh treh računalnikih odpreti vrata še v Windows Firewallu. Na koncu je treba dodati ime uporabnika, ki se bo lahko povezal s strežnikom, in označiti deljene datoteke. To storimo tako, da na strežniku na particiji D: ustvarimo mapo Backups2 in jo v uporabniškem vmesniku FileZille označimo kot Shared folder. Tako je bil v našem primeru

pripravljen strežnik, ki je hranil slike, ustvarjene s programom Norton Ghost, na dveh različnih lokacijah: mapi Backups in mapi Backups2.

Nato lahko program Norton Ghost namestimo tudi na drugi javni računalnik. Za razliko od prvega pri namestitvi na drugi računalnik ni treba preverjati gonilnikov in izdelati pogonskega CD-ja, saj sta oba testna računalnika strojno enaka. To pomeni, da sta sestavljena iz istih strojnih komponent, ki uporabljajo iste gonilnike. Zato lahko uporabljamo en pogonski CD za oba računalnika. Ko so oba javna računalnika in strežnik pripravljeni, se lahko posvetimo izdelavi slike trdega diska. To storimo tako, da na prvem testnem računalniku poženemo program Norton Ghost. Nato na uporabniškem vmesniku programa kliknemo na zavihek Home. Tu se odločimo za možnost Run or Manage Backups. Ko se pojavi novo okno, izbremo Define New in tako označimo nov posel. Nato v naslednjem oknu izbremo možnost Back up my Computer in pritisnemo na gumb Next. Pojavi se novo okno, v katerem so prikazane particije trdega diska. Ker smo imeli na testnih računalnikih samo eno particijo C:, kliknemo nanjo in jo tako označimo. Nato je treba označiti tip zaščitne kopije (*angl. backup*). Norton Ghost tu ponuja dve možnosti. Prva Recovery Point Set ob prvem zagonu ustvari sliko celotnega izbranega diska. Nato ob vsakem novem poslu ustvarjanja zaščitne kopije istega diska ustvari samo tako imenovano Incremental Recovery Point, ki vsebuje samo »razlike« od zadnje celotne zaščitne kopije. Ta možnost je priporočena, saj tako porabimo manj pomnilniškega prostora na računalniku, kjer shranjujemo slike trdega diska. Druga možnost Independent Recovery Point pa vsakič ustvari celotno sliko trdega diska. Izbrali smo prvo, priporočeno možnost. Zatem kliknemo na gumb Next. Naslednje okno, ki se pojavi v uporabniškem vmesniku, je okno, kjer določimo cilje za shranjevanje slik. V polju Folder Field kliknemo na gumb Browse in označimo Network Places ter zatem še strežniški računalnik, ki smo ga poimenovali Strežnik. S pritiskom na računalnik Strežnik se odpre še deljena mapa Backups, ki jo označimo. Zatem Norton Ghost zahteva avtentifikacijo na oddaljenem računalniku, zato je treba vpisati uporabniško ime in geslo administratorskega uporabnika na oddaljenem računalniku. To storimo v oknu Network Credentials. Zatem program Norton Ghost ponuja možnost poimenovanja slike. Privzeto se imenom računalnika, katerega sliko trdega diska ustvarimo, doda črka diska, v našem primeru TESTNI1_C_Drive001.s2i. Naslednja inkrementalna slika se imenuje TESTNI1_C_Drive001_i001.s2i, naslednja TESTNI1_C_Drive001_i002.s2i in tako naprej. Imena smo pustili kar takšna, kot so privzeta, saj dobro opisujejo sliko diska. Kot dodatno stopnjo varnosti Norton Ghost ponuja še možnost Offsite Copy, s katero lahko prenesemo sliko še na drugo oddaljeno lokacijo. V našem primeru je bila to mapa Backups2, dosegljiva preko FTP storitve. S pritiskom na gumb Add se odpre še eno polje, kamor lahko vpišemo naslov FTP-strežnika, in pot do mape, ki jo uporablja FTP-strežnik. Tudi tu je bilo treba vpisati uporabniško ime in geslo, s to razliko, da je na tem mestu treba vpisati ime in geslo za uporabnika FTP-storitve, ki smo ga predhodno nastavili na strežniku. Nato označimo še gumb Enable Offsite Copy. S pritiskom na gumb Next se pojavi naslednje okno uporabniškega vmesnika – Options. Tu lahko nastavimo še stopnjo stiskanja datotek. Mogoče je izbrati med naslednjimi vrednostmi: None, Standard, Medium in High. Na tej točki je odvisno, česa imamo na voljo več, ali časa ali pomnilniškega prostora. S pritiskom na možnost None se slika sicer hitro ustvari, vendar je skoraj iste velikosti kot disk, ki ga kopiramo. Najboljše razmerje ponuja možnost Standard, saj se je slika v velikosti 40 GB ustvarila in prenesla na oddaljeno lokacijo v 20 minutah, zasedla pa je 4.4 GB. Naslednja možnost, ki smo jo obkljukali v oknu Options, je bila Verify Recovery Point after Creation, ki preveri, ali se je slika diska zapisala pravilno in ali jo je možno obnoviti. Če temu ni tako, Norton Ghost izpiše sporočilo o napaki. V tem oknu nastavimo tudi hitrost ustvarjanja zaščitne kopije s premikanjem drsnika bližje vrednostim Fast ali Slow. Če bi drsnik premaknili

bližje Fast, bi se slika diska ustvarila hitreje, vendar pa bi računalnik zasedal več virov, kar bi za uporabnika pomenilo počasnejše odzivanje računalnika. S premikom drsnika bližje Slow je situacija ravno obratna. V tem oknu nastavimo še hitrost prenašanja slike do obeh oddaljenih lokacij s pritiskom na gumb Enable Network Throttling in vpisom največje dovoljene hitrosti prenosa. Tudi tu je situacija podobna kot pri določitvi hitrosti ustvarjanja slike. Počasnejši kot je prenos, bolj je računalnik odziven za uporabnika, na primer brskanju po spletu. Če pa določimo višjo hitrost prenosa, se kaj kmalu lahko zgodi, da uporabnik občuti posledice – počasnejše odzivanje brskalnika in nalaganja spletnih strani. S pritiskom na gumb Next se prikaže še zadnje okno. V tem oknu izbremo možnost Schedule, ki ponuja možnost označitve, kdaj oziroma ob katerih dnevih in urah se (inkrementalna) slika ustvari samodejno. Zatem kliknemo gumb Next. S tem se prikaže okno, v katerem so zapisane vse možnosti, ki smo jih izbrali za določeno sliko trdega diska. Izbrali smo možnost Schedule, zato se ustvarjanje zaščitne kopije začne ob določenih dnevih in urah, ki jih lahko izberemo. Ker pa smo hoteli ustvariti sliko takoj, se v tem zadnjem oknu izbre možnost Run Backup Now. S tem poženemo postopek ustvarjanja slike. Ko se je slika ustvarila in uspešno prenesla v mapo Backups na strežniku, Norton Ghost prične še s postopkom Offsite Copy, v našem primeru na FTP-strežnik. Ob uspešnem zaključku Norton Ghost uporabnika obvesti, da se je slika uspešno ustvarila, če je bila pred tem izbrana možnost Verify Recovery Point After Creation. Tako je uporabnik lahko prepričan, da se je slika trdega diska uspešno ustvarila. Ko je slika trdega diska ustvarjena in spravljena na strežniku, se lahko lotimo obnove sistema. Na obeh testnih računalnikih lahko ustvarimo preprosto tekstovno datoteko in jo spravimo na namizje. Zatem ponovno zaženemo prvi testni računalnik tako, da v CD-enoto vstavimo zagonski CD, s katerim lahko dostopamo v okolje Recovery. Na zaslonu se prikaže uporabniški vmesnik tega okolja.

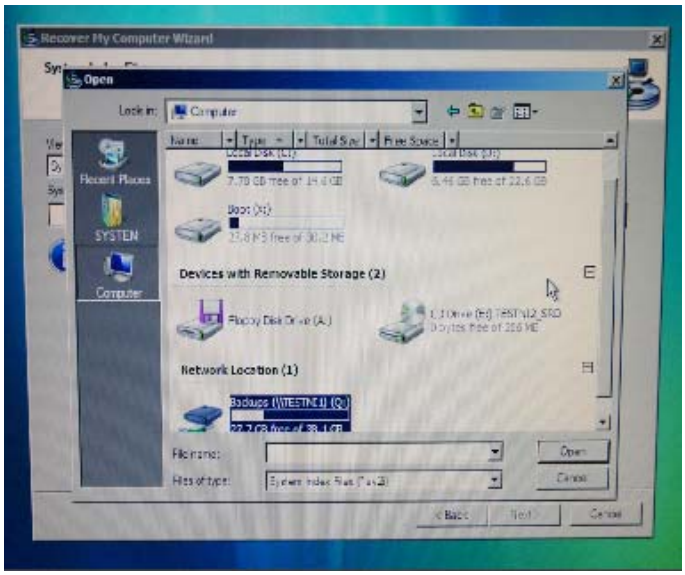
Slika 15: Recovery (obnovitveno) okolje, pognano z zagonskega CD-ja.

Ker smo imeli sliko trdega diska spravljeno na računalniku, ki je služil kot strežnik, je Norton Ghost zahteval, da se iz mape na strežniku naredi mrežni disk ali Network Drive. To storimo tako, da v okolju Recovery najprej kliknemo na zavihek Network. Iz menija izberemo opcijo Map a Network Drive. Postopek najprej zahteva, da se dodeli črko, ki bo predstavljala

mrežni disk. Ker smo imeli na testnem računalniku samo en disk z eno particijo C:, smo si za omrežni disk izbrali črko Q:. Nato v polju Folder pritisnemo gumb Browse, ki odpre okno, preko katerega lahko dostopamo do oddaljenih računalnikov. Z izbiro in pritiskom na besedo Network Neighborhood se pojavi seznam, ki je v našem primeru obsega oba testna računalnika z imenom Testni1 in Testni2 in strežnik, ki smo ga poimenovali Strežnik. Ker smo imeli sliko na strežniku, izberemo računalnik Testni1. Z izbiro računalnika se okolje Recovery vrne v prvo okno opisanega postopka. Treba je le še vpisati ime mape, v kateri je bila spravljena slika diska. Tu imamo dve možnosti, saj smo sliko diska ustvarili v dveh ločenih mapah Backups in Backups2, ki je mapa, ki pripada FTP-strežniku. Odločili smo se za mapo Backups. Tako v polje Browse dodamo še ime mape. Celoten zapis je izgledal takole //Strežnik/Backups. Čez nekaj sekund se na zaslonu prikaže sporočilo o uspešnem pripenjanju mrežnega diska.

Slika 16: Pripenjanje omrežnega diska v okolju Recovery.

Nato kliknemo na zavihek Recover my Computer. Okolje Recovery privzame, da se bo slika prenesla iz lokalnega računalnika, zato je treba v polju View by izbrati možnost System. S pritiskom na gumb Browse se odpre okno, podobno tistemu, ki ga dobimo s pritiskom na ikono My Computer v operacijskem sistemu Windows. V tem oknu smo izbrali ikono, ki je predstavljala omrežni disk Q:, in z dvoklikom na ikono Q: se je prikazala vsebina mrežnega diska.



Slika 17: Omrežni disk, ki je vseboval sliko trdega diska.

Tu izberemo datoteko Testni1_C_Drive001.v2i, ki predstavlja sliko lokalnega trdega diska C:, in kliknemo na gumb Next. Postopek nadalje zahteva, da si izberemo trdi disk, na katerega želimo sliko prenesti. V našem primeru je bil to lokalni disk C:. Nato kliknemo na gumb Next, ki pri tem postopku prikaže še zadnje okno, v katerem so zapisane vse zgoraj izbrane opcije. Bistveno pa je, da to zadnje okno prikaže ime slike diska in trdi disk, na katerega želimo sliko prenesti. S pritiskom na gumb Finish sprožimo postopek pisanja slike diska na lokalni trdi disk. Po približno desetih minutah se v okolju Recovery pojavi obvestilo o uspešnem postopku zapisovanja slike na trdi disk. Zatem vzamemo zagonski CD iz CD-enote in ponovno poženemo računalnik. Operacijski sistem se je naložil brez težav, pa tudi tekstovne datoteke, ki smo jo pustili na namizju, ni bilo več. Tako smo bili lahko prepričani, da se je slika diska brez težav prenesla na testni računalnik. Enak postopek ponovimo tudi na drugem testnem računalniku z imenom Testni2, vendar za njegov trdi disk ni treba napraviti slike, saj sta bila oba testna računalnika strojno enaka, zato lahko uporabimo kar sliko naprave s prvega testnega računalnika. Tudi na drugem računalniku je postopek uspel. Nato preizkusimo še delovanje programske opreme, naložene na oba računalnika, ki je v našem primeru delovala brez napak [11].

3. USTVARJANJE IN PRENAŠANJE SLIKE TRDEGA DISKA S POMOČJO OPERACIJSKEGA SISTEMA LINUX

V tem poglavju bom opisal postopek, kako s pomočjo operacijskega sistema Linux, TFTP-strežnika in nalagalnika GRUB lahko ustvarimo aplikacijo, ki posnema delovanje programske opreme Norton Ghost. Z njeno pomočjo lahko uporabnik naredi sliko trdega diska računalniškega sistema, nato pa to sliko spravi na strežniku. Če računalnik ne dela, lahko administrator s pomočjo zagonske diskete ali zagonskega CD-ja požene aplikacijo, ki prepiše vsebino slike na pomnilno napravo. Takšen način pa se lahko uporabi tudi za posnemanje programske opreme, ki temelji na tehnologiji naloži in obnovi. Pri nastavitvi operacijskega sistema Linux (katerakoli distribucija), je treba disk razdeliti na particije. Med te spada tudi particija, imenovana /usr, ki je namenjena »navadnim« uporabnikom (uporabniki, ki nimajo administratorskih pravic) operacijskega sistema. Velikost te particije lahko omejimo na velikost, ki bo dovoljevala prenos na in iz strežnika v zelo kratkem času. V našem primeru smo velikost particije /usr omejili na 2 GB in s tem dosegli, da se je slika te particije zapisala na trdi disk v treh

minutah. Uporabniki največkrat potrebujejo javne računalnike za brskanje po spletu, pisanje raznih datotek z urejevalniki besedil in podobno. Vsi ti programi so lahko posneti na drugih particijah. Zato lahko omejimo velikost /usr particije, saj je namenjena shranjevanju datotek uporabnikov, te pa so večinoma zelo majhne. Po določenem času lahko to particijo obnovimo s sliko, ki je shranjena na strežniku, in tako dobimo /usr particijo, kakršna je bila ob inštalaciji operacijskega sistema. Isti princip je lahko uporaben za obnovitev celotnega diska iz slike, ki si jo lahko izberemo.

Preden bom opisal sam način izdelave omenjene aplikacije, naj na kratko opišem še pojme, vgrajene programe in storitve, ki sem jih moral spoznati, preden sem lahko izdelal omenjeno rešitev.

3. 1. Vgrajeni program dd in organizacija strojnih naprav v operacijskem sistemu Linux

Program dd, ki je vgrajen v Linux operacijske sisteme, pomeni disk dump. Program dd je sposoben brati iz datotek in pisati vanje ali v pomnilne naprave (block devices) – to so naprave, ki omogočajo pisanje in branje več blokov podatkov hkrati. Tipičen način uporabe programa dd je naslednji:

dd if=(datoteka oziroma pomnilna naprava) of=(datoteka oziroma pomnilna naprava)

Program dd deluje tako, da mu kot parametre podamo vhodno datoteko, iz katere prebere podatke (blok za blokom), in izhodno datoteko, v katero podatke zapiše. To naredimo tako, da ukazu dd podamo parametra if in of. Parameter if je kratica za besedno zvezo input file, v slovenščini izvorna datoteka. Parameter of pa je kratica za besedno zvezo output file, kar lahko prevedemo kot ponorna datoteka. Poleg obeh opcij je treba napisati ime datoteke oziroma pomnilne naprave, iz katere beremo oziroma v katero se zapišejo podatki. Ker pa so v vseh distribucijah Linux operacijskega sistema pomnilne naprave obravnavane kot navadne datoteke, je mogoče kot izvorno in ponorno datoteko določiti pomnilno napravo. V operacijskem sistemu Linux so vse strojne naprave, ki sestavljajo računalnik, dosegljive v mapi /dev (devices). Trdi disk se v operacijskem sistemu Linux naslavlja kot hda ali sda. Diski, ki jih operacijski sistem prepozna in pripne preko vodila IDE, se imenujejo hd, kjer je hd okrajšava za trdi disk (*angl. **h**ard **d**isk*). Če imamo v računalniku en trdi disk, bo operacijski sistem ta trdi disk prikazal kot /dev/hda. V primeru, da imamo v računalniku dva trda diska, se bo prvi trdi disk (*angl. primary master*) prikazal kot /dev/hda, drugi priključeni trdi disk (*angl. primary slave*) pa se bo prikazal kot /dev/hdb. Particije diskov operacijski sistem Linux prikazuje kot /dev/hda1, /dev/hda2 in tako naprej.

Če imamo v računalniku tako imenovane SATA (priključene preko Serial-ATA vodila) trde diske, se le-ti prikažejo kot /dev/sda, /dev/sdb in tako naprej. Tudi tu se particije prikažejo z zaporedno številko particije, torej kot /dev/sda1 – prva particija, /dev/sda2 – druga particija in podobno dalje.

Če imamo v računalniku priključena dva trda diska in imamo na prvem trdem disku nameščen operacijski sistem in programsko opremo, lahko vsebino trdega diska zapišemo na drugi trdi disk s programom dd. To storimo z naslednjim ukaznim nizom:

dd if=/dev/hda (ali sda) of=/dev/hdb (ali sdb)

Edini pogoj pri uporabi tega programa je, da sta diska enako velika in uporabljata isto vodilo. Tako lahko ustvarimo kopijo celotnega trdega diska na drugem trdem disku. Pri tem ni nujno, da je disk, na katerega pišemo, prazen, saj ukaz dd ustvari kopijo, tako da zapiše vsak sektor diska, iz katerega pišemo. Prav tako zapiše na ciljni disk vse sektorje in s tem prepiše prejšnjo vsebino. Tako se prepiše celotna vsebina diska, med drugim tudi MBR (Master Boot Record), tabela particij in drugi pomembni podatki. V tem primeru bi lahko po izvršitvi ukaza dd kot trdi disk, iz katerega se požene operacijski sistem, označili disk hdb, saj je hdb natančna kopija prvega trdega diska. Operacijski sistem bi se naložil in deloval brez težav. Kot ponorno datoteko bi lahko ukazu dd pridružili navadno datoteko in ne pomnilne naprave. Program dd pri kopiranju ignorira datotečni sistem, če bere iz pomnilne naprave, in ustvari sliko (*angl. raw image*), ki se prikaže kot datoteka brez končnice. Ta datoteka je do bajta natančna kopija pomnilne naprave. Ravno zaradi te značilnosti lahko program dd izkoristimo za ustvarjanje slik pomnilnih naprav v datoteke, nato pa te datoteke shranimo na mesto, iz katerega jih lahko zapišemo nazaj na pomnilno napravo.

3. 2. Glavna številka naprave in številka particije

Naprave so v operacijskem sistemu Linux razdeljene v skupine, imenovane glavne številke naprave (*angl. major device number*). Vsi SATA trdi diski imajo tako pridruženo glavno številko naprave 8, vsi IDE trdi diski pa imajo glavno številko naprave 3. Vsaka naprava iz posamezne skupine ima tudi svojo številko particije (*angl. minor device number*). Trdi disk /dev/sda, nameščen v računalniku, ima na primer številko particije 0. Operacijski sistem Linux uporablja glavno številko naprave in številko particije kot način identifikacije strojnih naprav jedru operacijskega sistema (*angl. kernel*). Kot je bilo že omenjeno, so naprave v operacijskem sistemu Linux predstavljene kot datoteke. Glavna številka naprave in številka particije datoteke oziroma naprave sta potrebni, da lahko jedro dostopa in naslavlja strojne naprave, med njimi tudi trde diske. Z ukazom v lupini ls -l /dev/hda (sda) dobimo izpis:

brw-rw----- 1 root disk 3 , 0 …..... /dev/hda

V tem primeru sta par glavna številka naprave in številka particije, 3 in 0.

3. 3. TFTP, BOOTP, UDP-protokol

Za prenos slik med strežnikom in ciljnimi računalniki smo uporabljali storitev TFTP. TFTP (Trivial File Transfer Protocol) je v uporabi že od 80. let prejšnjega stoletja, iz tega protokola so kasneje izpeljali tudi FTP-protokol (File Transfer protocol). TFTP-storitev se uporablja za prenose datotek po mreži. TFTP uporablja UDP (User Datagram Protocol), pogosto v kombinaciji z BOOTP (Bootstrap Protocol), kar drži tudi v našem primeru.

UDP je protokol, ki se uporablja za prenos paketov med parom vtičev (*angl. socket*), ki se v primeru protokola UDP imenujejo datagrami. Prenos tipično poteka v obe smeri, torej od strežnika k odjemalcu in obratno. UDP je protokol transportne plasti, uporablja pa se v kombinaciji z IP-protokolom, ki leži na plasti nižje, torej na omrežni plasti. UDP je tako imenovan nepovezovalni protokol za prenašanje paketov podatkov. Nepovezovalni je zato, ker odjemalec in strežnik med sabo ne vzpostavita povezave (*angl. handshake*), pač pa prenos poteka tako, da strežnik pošilja podatke do odjemalca. Strežnik pri UDP-protokolu ne preverja, ali je odjemalec pakete dobil, zato lahko prenos podatkov teče hitreje, saj odjemalec ne čaka na

potrditev, da se je vsak posamezni paket uspešno prenesel. Razlog, da lahko UDP-način prenosa paketov uporabljamo pri storitvi TFTP, je v tem, da je v protokolu TFTP vsebovano sporočilo o napaki. Tako smo lahko kljub uporabi protokola UDP prepričani v pravilen prenos datoteke, v našem primeru slik trdega diska.

BOOTP je protokol, ki se uporablja zato, da je računalnik sposoben dobiti svoj IP-naslov in oziroma ali zagonsko (*angl. bootstrap*) datoteko. Tudi protokol BOOTP uporablja za prenos podatkov UDP-protokol. BOOTP poišče parametre, potrebne za zagon računalniškega sistema. Največkrat se uporablja pri postopku mrežnega ali network zagona računalnika v kombinaciji s storitvijo TFTP, ki prenese datoteko bootstrap na računalnik.

3. 4. Opis delovanja protokola TFTP

Pri protokolu TFTP lahko odjemalec zahteva:

RRQ (read request): zahteva po branju oziroma prenos datoteke s strežnika.
WRQ(write request): zahteva po prenosu datoteke na strežnik.

Med samim prenosom, lahko obe strani, torej odjemalec in strežnik pošiljata:

DATA: podatki, ki se prenašajo med strežnikom in odjemalcem. Vsak skupek ali blok podatkov ima svojo oznako Dn, pri čemer je n naravno število.

ACK: potrditev sprejema s številko, ki pripada podatkovnemu bloku Dn.
ERROR: pošiljanje sporočil o napaki če pride do nje.

Podatkovni (DATA) bloki so označeni od števila ena naprej z imenom Dn za njihovo vsebino. ACK uporablja za potrditev kar številko podatkovnega bloka. Če je bil blok D1 pravilno sprejet, se pošlje potrditev ACK1. V primeru zahteve po pisanju (prenosu) WRQ se pošlje potrditev s številom nič. Vsi podatkovni bloki Dn razen zadnjega so polni, zadnji blok, ki je lahko manjši, pa je identificiran z imenom Dlast.

3. 5. Zagonski proces računalnika

Zagonski proces računalnika je potreben zato, ker strojna oprema ne ve, kje leži operacijski sistem, niti, kako ga naložiti. Za to poskrbi poseben program, ki se imenuje bootstrap loader ali nalagalnik. Največkrat je to BIOS (Basic Input Output System). Naloga nalagalnika je, da poišče jedro operacijskega sistema, ga naloži v pomnilnik, sproži njegovo izvajanje ter ga zažene. Večkrat se zgodi, da preprost nalagalnik poišče bolj zahteven zagonski program in ga naloži v pomnilnik. Naloga drugega, kompleksnejšega zagonskega programa, je, da naloži jedro operacijskega sistema. Dogodek reset (zagon ali vklop računalnika) postavi programski števec na določeni naslov v pomnilniku, kjer je zapisan program za nalaganje. Ta program je pomnjen v ROM-pomnilniku, saj je ob tem času lahko RAM-pomnilnik v neznanem stanju.

Zagon računalnika se začne z diagnostiko, ki preveri stanje stroja. Ta diagnostika se imenuje POST (Power On Self Test) in preveri osnovno delovanje strojne opreme, ki sestavlja računalniški sistem. BIOS zatem pregleda pomnilne naprave in poišče tisto, ki je zagonska (*angl. bootable*). V primeru, da takšne naprave ne najde, sledi sporočilo o napaki in zagonski proces se zaustavi. Zagon se nadaljuje z inicializacijo registrov centralne procesne enote, krmilnikov

naprav in vsebine pomnilnika, šele nato sledi nalaganje operacijskega sistema. Operacijski sistem se naloži s programom Bootstrap loader. Ta program naloži »prvi program«, ki je običajno jedro operacijskega sistema. Ko BIOS najde zagonsko napravo, naloži njen zagonski sektor (Boot Sector) in ga sproži. V primeru trdega diska je to MBR (Master Boot Loader – sektor 0). Koda, naložena v MBR, preveri tabelo particij in v njej poišče aktivno, torej particijo, iz katere se bo zagnal operacijski sistem. Če takšno particijo najde, naloži koda v MBR zagonski sektor aktivne particije in sproži njeno izvajanje. Zagonski sektor particije (VBR – Volume Boot Record) je specifičen za posamezni operacijski sistem. Največkrat je naloga kode zagonskega sektorja nalaganje in poganjanje jedra, lahko pa se zgodi, da se v VBR nahaja sekundarni zagonski nalagalnik. Poznamo več različnih sekundarnih nalagalnikov, ki so specifični za dani operacijski sistem. Najbolj znani oziroma uporabljani so GRUB (Grand Unified Boot Loader), Lilo (Linux Loader) in NTLDR (NT Loader). Naloga sekundarnih zagonskih nalagalnikov je, da omogoča izbiro particije, iz katere se naloži operacijski sistem, zato se sekundarni nalagalniki imenujejo tudi zagonski upravniki (*angl. boot managers*). Lastnost omogočanja izbire particij posledično omogoča nalaganje različnih operacijskih sistemov, ki so lahko nameščeni na enem trdem disku. Za svoje delo sem si izbral nalagalnik GRUB, ki omogoča izbiro ter zagon jeder Linux, izbiro in zagon jeder, ki niso Linux in pa nastavljanje konfiguracije interaktivno, torej ob samem zagonu. Prva faza (*angl. stage 1*) GRUB-nalagalnika tipično leži v MBR trdega diska. Prva faza naloži drugo fazo (*angl. stage 2*), ki se lahko nahaja drugje. Faza dve je tista, ki prebere konfiguracijsko datoteko grub.conf, pokaže uporabniški vmesnik in nadaljuje z nalaganjem jedra operacijskega sistema, ki je lahko distribucija Linux ali kakšen drug operacijski sistem. Po nalaganju se sistemski zagon začne s tem, da se inicializira jedro operacijskega sistema. V osnovi je naloga jedra, da poskrbi za komunikacijo med procesi (programi v izvajanju) in strojno opremo. Lahko rečemo, da jedro poskrbi oziroma zagotavlja, da strojna oprema počene to, kar od nje zahtevajo programi v izvajanju. Med drugim jedro poskrbi tudi za preizkus pomembnih oziroma ključnih naprav, kot sta centralna procesna enota in pomnilnik. Jedro skrbi tudi za preizkus strojnih podsistemov, kot so vhodno-izhodna vodila, omrežni vmesniki in CD-ROM.

Ko GRUB zažene jedro, mu sporoči podatke o drugih delih operacijskega sistema, ki se nahajajo v RAM-pomnilniku. To naredi s pomočjo datoteke initrd (init ram disk), ki je osnovni (root) datotečni sistem in poskrbi za pripenjanje datotečnega sistema. Nalaganje se nadaljuje z akcijami procesa init. Init je predhodnik vseh ostalih procesov, vendar svoje zadolžitve, razen te, da »seje« ostale procese, nima. Init do jedra dostopa preko sistemskih klicev. Skrbi za zagon skript, ki postanejo procesi. Prednost uporabe skript pri zagonu je ta, da jih lahko spreminjamo in tako odkrijemo napake, ki bi lahko prekinile zagonski proces in povzročile neuporabnost računalniškega sistema.

Ko razumemo delovanje programa dd, storitve TFTP in zagonski proces računalnika, lahko nadaljujemo s postavljanjem sistema za preprečevanje izpada in zagotavljenje varnosti javnih računalniških sistemov.

3. 6. Izvedba rešitve

Cilj lahko opišemo kot sistem, ki temelji na soritvi TFTP in mrežnem zagonu računalnika. Računalnik takoj po zagonu prične z izvajanjem aplikacije, s katero lahko prenašamo sliko trdega diska z računalnika na strežnik ali obratno.

Javni računalniki imajo večinoma samo en fizični trdi disk. Zato bi bilo nemogoče napraviti sliko diska, jo shraniti na lokalni disk in jo kasneje obnoviti z lokalnega trdega diska, ki ga uporablja operacijski sistem. Prav tako se večkrat lahko zgodi, da je računalnik tako hudo

okvarjen, da ni sposoben naložiti operacijskega sistema. S postopkom mrežnega zagona računalnika (*angl. network boot*) se postavimo med strojno opremo in operacijski sistem. Z drugimi besedami, naložimo sliko okrnjenega operacijskega sistema, ki vsebuje le tiste operacije in storitve, ki jih potrebujemo. Tako računalnik niti ne poskuša naložiti operacijskega sistema z lokalnega trdega diska. Opisani postopek bi lahko bil uporaben tudi za namestitev operacijskega na vgrajene sisteme, ki imajo v splošnem zelo majhen pomnilnik (npr. razne medicinske naprave).

Ker smo imeli na voljo za preizkus rešitve dva starejša računalnika, ki sta imela 40 GB diska na IDE-vodilu, smo se odločili za nekoliko starejšo različico operacijskega sistema Linux, saj bi novejše različice imele težave pri prepoznavanju trdega diska. Jedra operacijskega sistema Linux pred verzijo 2.6 so imela namreč naložene gonilnike za prepoznavo in pripenjanje IDE-diskov. Isto rešitev bi lahko uporabil tudi na novejših računalnikih, ki imajo navadno trde diske priključene preko SATA-vodila. Paziti bi morali le na to, da bi izbrali tudi novejšo različico operacijskega sistema.

Postopek začnemo tako, da na računalnik, ki se uporablja kot strežnik, namestimo operacijski sistem. V našem primeru je bila to distribucija operacijskega sistema Linux, Red Hat 8.0. Pri postopku nameščanja je treba paziti, da je vsaj ena particija velika 30 GB, saj je namenjena shranjevanju slike trdega diska. Če bi za to particijo izbrali particijo /root, bi lahko imeli težave z delovanjem računalnika, zato izbremo particijo /usr. Pri postopku nameščanja pazimo na to, da je strežnikov IP nastavljen statično, kar omogoča, da ima strežnik ob vsakem zagonu enak IP. Postopek je podoben že opisanemu v poglavju o programski opremi Deep Freeze. Tudi tu smo sistem načrtovali tako, da sta bila oba računalnika, strežnik in testni računalnik, priključena na isti usmerjevalnik, ki je omogočal storitev DHCP. Pri namestitvi operacijskega sistema je treba paziti tudi na to, da odpremo vrata 69, ki jih uporablja storitev TFTP. Ko je namestitev operacijskega sistema končana, poskrbimo za namestitev TFTP-strežnika na računalnik, ki se uporablja kot strežnik. Na spletu poiščemo tako imenovan rpm (Red Hat Package Manager), s pomočjo katerega namestimo TFTP-strežnik. Po prenosu paketa rpm odpremo bash lupino operacijskega sistema in vpišemo ukaz:

rpm -i tftp-server-0.23-3.i386.rpm

S tem ukazom namestimo TFTP-strežnik. Pri ukazu rpm je treba dodati stikalo -i, ki pomeni install. Ko se namestitev konča, se v lupini najprej postavimo na particijo /usr in vpišemo ukaz *mkdir /tftpboot*. Z ukazom *mkdir* na particji /usr ustvarimo mapo, ki je namenjena odložišču za slike, hkrati pa v to mapo uvrstimo tudi datoteke, ki jih testni računalnik potrebuje za postopek mrežnega zagona (*angl. network boot*). Nato spremenimo pravice za dostop do mape z ukazom *chown nobody:nobody /usr/tftpboot*. S tem ukazom določimo, da imajo do te mape dostop vsi uporabniki vseh uporabniških skupin. To je tudi privzeta nastavitev za TFTP-strežnik. Če tega ne bi storili, bi lahko imeli težave z dostopom in pisanjem datotek v to mapo. Hkrati je računalnik, ki se uporablja kot strežnik, v primeru javne uporabe takšnega sistema lociran drugje kot javni računalniki, tako da se za varnost dostopa do teh datotek ni bati.

Naslednji korak je, da v mapi /etc/xinetd.d prilagodimo vsebino datoteke tftp. Xinetd je okrajšava za eXtended Internet Deamon. Deamon bi lahko opisali kot program, ki teče v ozadju in na katerega uporabniki računalnika neposredno ne vplivajo. V tej mapi se torej nahajajo datoteke, ki skrbijo za pravilno delovanje storitev, kot so FTP, Telnet ali TFTP. V datoteki tftp je osnovni zapis naslednji:

```
service tftp
{
        socket_type=  dgram
        protocol= udp
        wait= yes
        user= root
        server= /usr/sbin/in.tftp
        server_args= -s /tftpboot
        disable= yes
        per_source= 11
        cps= 100 2
        flags= IPv4
}
```

Edine spremembe, ki jih napravimo, so, da spremenimo parameter disable=yes v no. S tem zagotovimo delovanje storitve TFTP, ki je bila do te spremembe sicer nameščena, vendar onemogočena. Druga ključna sprememba pa je dodatek stikala -c v vrstico server_args, ki je po popravku izgledala takole:

```
server_args= -c -s /tftpboot
```

Z dodatkom tega stikala omogočimo ustvarjanje datotek v mapi tftpboot. Brez tega dodatka bi bilo pošiljanje slike s testnega računalnika na strežnik onemogočeno, saj v mapi /tftpboot ne bi mogli pisati datotek. Nato spremembe shranimo in poženemo bash lupino operacijskega sistema. V lupini zaženemo ukaz */etc/rc.d/init.d/xinetd reload*, s katerim se ponovno požene storitev xinetd s spremembami, ki smo jih vpisali. Brez ponovnega zagona se napravljene spremembe ne bi poznale in imeli bi težave pri uporabi storitve TFTP.

Nato se lotimo namestitve operacijskega sistema Red Hat 8.0 še na testni računalnik. Pri tej inštalaciji pustimo vse prednastavljene nastavitve. Računalnik smo med namestitvijo Red Hat 8.0 nastavili tako, da je svoj IP dobil dinamično. To je tudi privzeta nastavitev pri inštalaciji.

Ko se postopek namestitve zaključi, s namestimo še TFTP client storitev, ki omogoča povezovanje s TFTP-strežnikom in prenos datotek. Da se prepričamo, da storitev TFTP deluje, lahko na testnem računalniku ustvarimo tekstovno datoteko z imenom Testna in jo pošljemo na strežnik. To storimo tako, da se v lupini prestavimo v mapo, v kateri je tekstovna datoteka, nato pa sem vtipkamo ukaz, ki se glasi:

```
tftp 192.168.1.11
tftp>ascii
tftp>put Testna testna
tftp>quit
```

Ko vnesemo prvo vrstico tftp 192.168.1.1, ki je klic po storitvi TFTP z IP-številom strežnika, se pojavi tako imenovan tftp prompt. Tu najprej vtipkamo način prenosa datoteke na strežnik. Storitev TFTP ponuja dva načina pošiljanja datotek, in sicer ASCII in BINARY. Napačen način prenosa lahko »uniči« poslano datoteko, tako da je na strežniku ne moremo odpreti in pogledati njene vsebine. Tekstovne datoteke se večinoma pošilja kot ascii datoteke,

medtem ko se z načinom binary prenašajo na primer datoteke, ustvarjene s programi za urejanje besedil, in podobno, v našem primeru tudi slike. Pri uporabi storitve TFTP imamo na voljo tudi dva ukaza, s pomočjo katerih prenesemo datoteko na strežnik oziroma z njega. Z ukazom *put* lahko pošljemo datoteko na strežnik, z ukazom *get* pa datoteko prenesemo s strežnika na računalnik. Pri obeh ukazih lahko poleg imena datoteke, ki jo pošiljamo, dodamo še ime datoteke, ki bo vidno po zaključku prenosa. Ko se prepričamo v delovanje storitve TFTP, lahko nadaljujemo s postopkom.

Naslednji korak je priprava datotek, s pomočjo katerih se je testni računalnik sposoben zagnati z mreže. Tu sta pomembni predvsem dve datoteki. Prva je jedro operacijskega sistema, druga pa datoteka initrd, ki jo jedro pripne kot začetni, osnovni (*angl. root*) datotečni sistem. Najprej se na testnem računalniku prijavimo v operacijski sistem kot administrator (*angl. root*). To omogoča dostop do vseh datotek, tudi sistemskih. Ko smo prijavljeni v operacijskem sistemu, poženemo ukazno lupino. Z ukazom *cd /boot*, se postavimo na zagonsko particijo trdega diska. Nato z ukazom *ls vmlinuz-$ (uname -r)* na zaslonu dobimo izpis datoteke, ki predstavlja jedro operacijskega sistema. S stikalom *-r* dosežemo, da se ime izpiše na standardnem izhodu, torej na zaslonu. Izpis je naslednji:

vmlinuz-2.4.18-3

Nato s storitvijo TFTP pošljemo jedro operacijskega sistema na strežnik. Celotni ukazni niz izgleda takole:

```
tftp 192.168.1.11
tftp>binary
tftp>put vmlinuz-2.4.18-3 vmlinuz
tftp>quit
```

Pri tem postopku smo jedro namerno primenovali v vmlinuz, saj tako dosežemo, da lahko več strojno enakih računalnikov zaženemo z istim jedrom. To pomeni, da se za serijo strojno enakih računalnikov lahko uprablja isti zagonski medij (CD-ROM, disketa).

Naslednji korak je izdelava datotečnega sistema, ki ga je jedro sposobno pripeti kot osnovni datotečni sistem. Tu je potrebno vključiti vse datoteke, ki vsebujejo ukaze in storitve, ki jih potrebujemo za prenos in nastajanje slike. Potrebujemo lupino bash, mrežne storitve (DHCP, TFTP), s katerimi je testni računalnik sposoben dobiti dinamični IP-naslov z DHCP-strežnika oziroma prenašati datoteke. Potrebujemo tudi programa dd, za ustvarjanje slike, in gzip, s katerim lahko velikost slike skrčimo in tako privarčujemo prostor na strežniku. Med pomembnejšimi ukazi, ki jih je potrebno vključiti, so bili tudi ukazi mknod, ki omogoča ustvarjanje bločnih datotek, in pa mount in insmod. Z ukazom mount sporočimo operacijskemu sistemu, da je datotečni sistem pripravljen za uporabo in ga pripnemo na določeno točko v datotečni hierarhiji. Ukaz insmod pa naloži potrebne module, med katerimi je bil v našem primeru najpomembnejši modul za mrežno kartico, in jih vstavi v jedro operacijskega sistema. V ta namen ustvarimo navadno tekstovno datoteko initrd.txt in vanjo zapišemo imena vseh datotek, ki jih potrebujemo (vsebina datoteke initrd.txt je v prilogi). Pri tem postopku je potrebno veliko pregledovanja, saj se je treba prepričati, da datoteke, ki omogočajo storitve in ukaze, obstajajo, oziroma so nameščene v operacijskem sistemu. Ko smo se prepričali, da datoteke obstajajo, v lupini poženemo ukaz:

dd if=/dev/zero of=initrd bs=1024 count=4096

S stikalom bs=1024 nastavimo velikost vhodnih in izhodnih blokov, ki jih zapisujemo, s stikalom count pa dosežemo to, da se prekopira samo določeno število vhodnih blokov, natančneje štirje. Velikost datoteke initrd je 4 MB. S parametrom if=/dev/zero ustvarimo bločno datoteko, ki je v našem primeru vsebovala same ničle. To storimo zato, da kasneje lahko pripnemo datotečni sistem.

Sledi opis postopka pripenjanja in pošiljanja datotečnega sistema:

- Datotečni sistem ustvarimo z ukazom *mkfs initrd*. Ko pritisnemo tipko ENTER, nas operacijski sistem opozori, da datoteka initd ni bločna naprava.
- V lupini se pojavi naslednje opozorilo: initrd is not a block special device. Proceed anyway (y, n)?
- S pritiskom na tipki y in ENTER sprožimo nastanek datotečnega sistema.
- Ko se postopek konča, si z ukazom *mkdir pripni* ustvarimo mapo, ki služi kot točka pripenjanja (*angl. mount point*).
- Nato z ukazom *mount -o loop initrd pripni/* pripnemo datoteke iz initrd v mapo pripni.
- Z ukazom *initrd.txt | cpio -pdm pripni* skopiramo vsebino datoteke initrd v mapo pripni.

Po izvršitvi tega ukaza bi z dostopom do mape pripni dostopali do pravkar ustvarjenega datotečnega sistema initrd. Z ukazom *mount -o loop* operacijskemu sistemu povemo, da je naprava, ki jo pripenjamo, psevdonaprava, ki naredi datoteko dosegljivo kot bločno napravo. Ko izvršimo ukaz *cpio*, nas operacijski sistem opozori, da datoteke /bin/obnovi, /bin/tftp in /lib/3c59x.o ne obstajajo. Razlog za to je, da skopiramo originalni datotečni sistem v »naš« datotečni sistem. Tako program tftp ni zapisan v mapi /bin/tftp, pač pa v mapi /usr/bin/tftp. Datoteka /bin/obnovi je skripta, s katero ustvarimo aplikacijo, ki jo lahko uporabnik uporablja samo s pritiskom na gumbe. Z drugimi besedami, kdorkoli lahko naredi sliko trdega diska ali uporabniške particije, ne da bi poznal ukaze, saj ga aplikacija vodi. Skripta obnovi je opisana v prilogi. Tretje opozorilo pa se nanaša na gonilnike mrežne kartice, ki so zapisani v datoteki /lib/modules/vmlinuz-2.4.18-3/kernel/drivers/net/3c59x.o in ne v datoteki /lib/3c59x.o. Da izvemo, kateri gonilnik uporablja mrežna kartica v računalniku, vtipkamo ukaz *lsmod*, ki pokaže vse module, ki jih računalnik uporablja. Zatem samo preberemo ime gonilnika, ki ga uporablja mrežna kartica, in ga dodamo v naš datotečni sistem. Obvestilo o napakah je tu normalno, saj je treba še skopirati dejanske datoteke v lasten datotečni sistem. To storimo z ukazom *cp* in v primeru obvestila o napaki tftp datoteke vtipkamo ukaz *cp -p /usr/bin/tftp pripni/bin/*. Enako storimo z ostalima datotekama, ki sta prikazali obvestila o napaki, le da pred kopiranjem skripte obnovi le-to naredimo zmožno zagona (*angl. executable*) z ukazom *chmod +x obnovi*. Zatem odpnemo (*angl. unmount*) mapo pripni, stisnemo datoteko initrd in jo pošljemo na strežnik. Zaporedje ukazov se glasi:

```
umount pripni/
gzip initrd
tftp 192.168.1.11
tftp>binary
tftp> put initrd.gz initrd.gz
tftp>quit
```

Naslednji in hkrati zadnji korak pa obsega izdelavo zagonskega medija, s katerim testnemu računalniku pokažemo pot do datotek vmlinuz in initrd na strežniku in inicializiramo skripto, s pomočjo katere pišemo s trdega diska oziroma na njega. Kot je bilo že omenjeno, je

večina logike nalagalnika GRUB zapisana v konfiguracijski datoteki grub.conf. Na testnem računalniku ustvarimo datoteko grub.conf, ki ima naslednjo obliko:

```
default=0
timeout=5
title=Obnovi sistem
        bootp
        tftpserver=192.168.1.11
        root (nd)
        kernel /vmlinuz rw root=/dev/ram ramdisk_size=4096 init=/bin/obnovi
        initrd /initrd.gz
```

Parameter default pomeni, koliko časa naj GRUB počaka, preden začne z nalaganjem operacijskega sistema. To lahko spremenimo s parametrom timeout, ki v našem primeru nalagalniku pove, da naj počaka pet sekund, preden začne z nalaganjem. Bootp je ukaz, s katerim računalnik dobi IP-naslov od DHCP-strežnika. Ukaz tftpserver pove nalagalniku GRUB, na katerem naslovu se nahaja strežnik tftp, s katerega se bo sistem zagnal. Ukaz root (nd) pa nalagalniku GRUB pove, da se operacijski sistem nahaja na mrežnem disku (nd pomeni network drive).

Ukaz kernel nalagalniku pokaže jedro operacijskega sistema, parametri pa pomenijo naslednje:

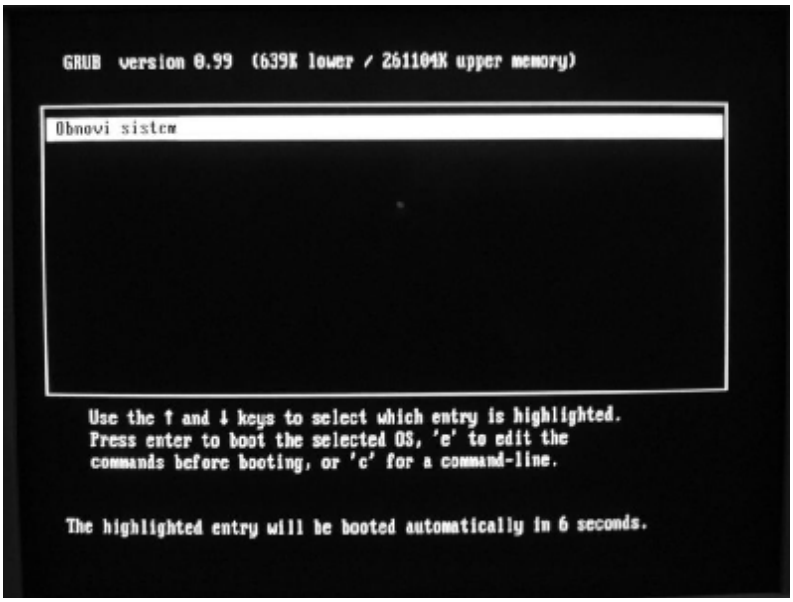
- parameter rw uporabimo, ker tako določimo pripenjanje datotečnega sistema s pisanjem v pomnilnik RAM,
- z root=/dev/ram nalagalniku sporočimo, kam naj pripne osnovni datotečni sistem,
- z ramdisk_size nalagalniku sporočimo velikost osnovnega datotečnega sistema,
- s parametrom init=/bin/obnovi določimo, da naj se kot prvi proces sproži skripta, s pomočjo katere se proži pisanje v sliko in iz nje nazaj v napravo,
- initrd uporabimo, da določimo datoteko, v kateri je zapisan osnovni datotečni sistem.

Nato na spletni strani GRUB poiščemo paket z nalagalnikom GRUB, ki ustreza verziji operacijskega sistema, ki ga uporabljamo. Ker je stisnjen s programom tar, ga moramo najprej razpakirati (*angl. decompress*). To storimo z ukazom *tar xzf grub-0.99.tar.gz*. Ko se postopek konča, se z ukazom *cd grub-0.99* prestavimo v mapo, v katero se je razpakiral nalagalnik GRUB. Zatem z ukazom *./configure –enable-preset-menu=../grub.conf –enable-3c90x* nastavimo nalagalnik GRUB tako, da omogoča uporabo mrežne kartice in pokaže meni, ki ga ustvarimo z datoteko grub.conf. Nato z ukazom *make* prevedemo kodo nalagalnika GRUB, da je sposoben uporabljati mrežno kartico, ki jo imamo v računalniku, prav tako pa v meniju pokaže naslov Obnovi sistem. Ker v testnem računalniku nismo imeli na voljo CD-zapisovalnika, smo ustvarili zagonsko disketo z ukazom, ki smo ga sprožili v lupini, tako kot vse prejšnje:

cat stage1/stage1 stage2/stage2 | dd of=/dev/fd0

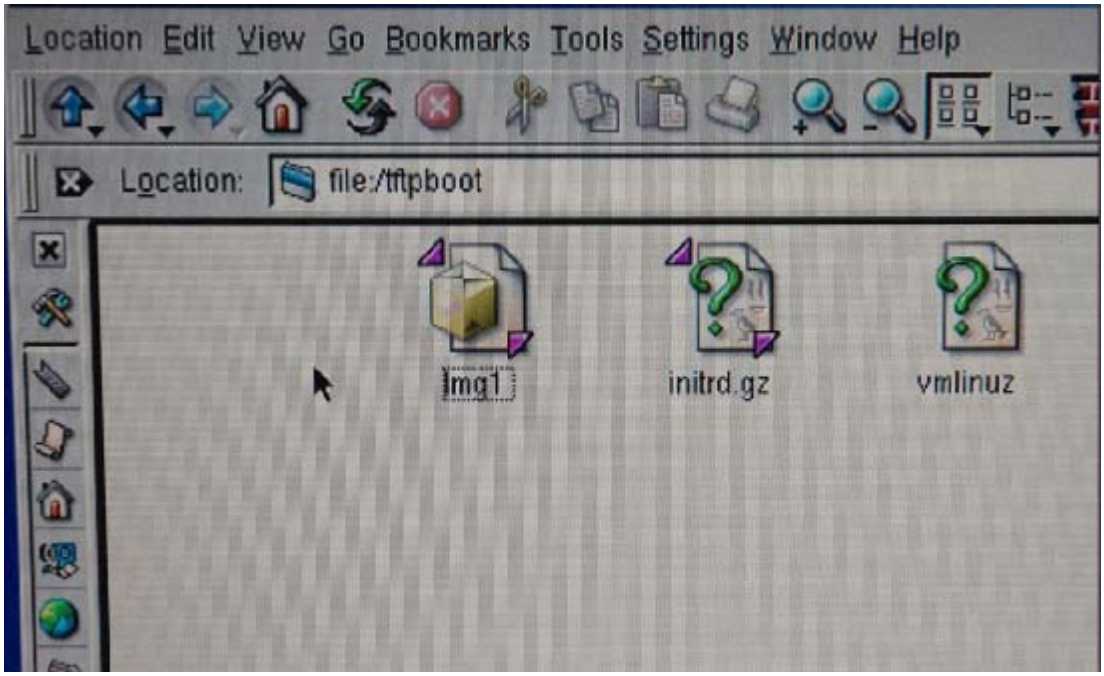
S tem se ustvari slika zagonske diskete, ki je sestavljena iz stika datotek stage1/stage1 in stage2/stage2, pri čemer sta datoteki stage1 in stage2 tisti, ki smo jih prevedli, tako da nalagalnik zna uporabljati mrežno kartico in se zagnati s pomočjo datotek na strežniku. Tako je postopek zaključen.

Preostane nam le še preizkus sistema. Da preizkusimo delovanje skripte, znova poženemo računalnik in v BIOS-u določimo disketo, ki smo jo ravnokar ustvarili, kot primarno zagonsko napravo. Nato znova poženemo računalnik, tokrat z vstavljeno disketo.

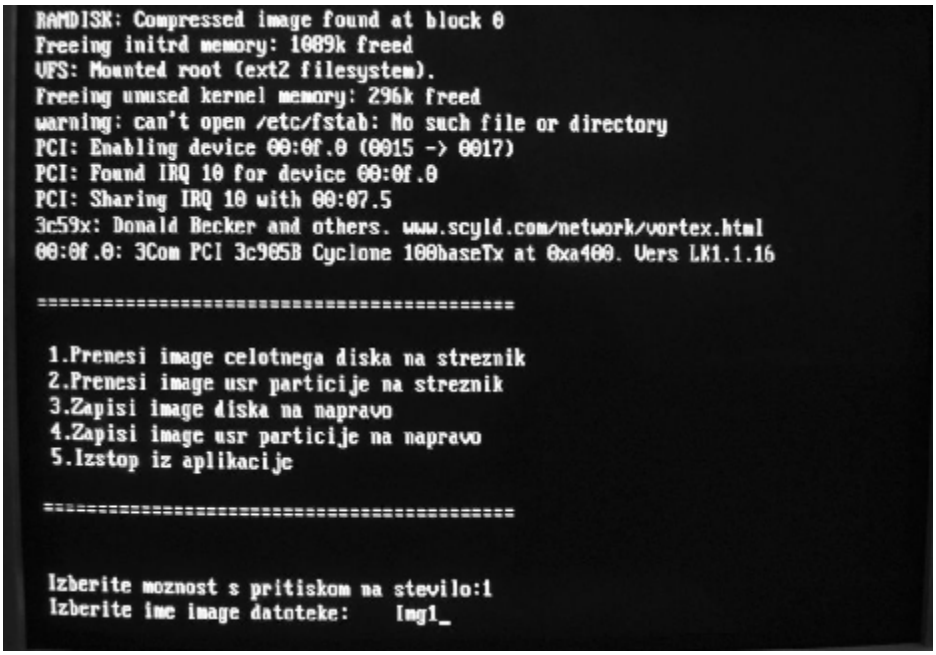


Slika 18: Zagon računalnika z mrežnega diska preko nalagalnika GRUB.

Zatem s pomočjo skripte ustvarimo sliko uporabniške particije in jo pošljemo na strežnik. Nato znova poženemo računalnik, tako da izvlečemo zagonsko disketo in pustimo da se operacijski sistem naloži z lokalnega trdega diska. V sistem se prijavimo kot administrator in na /usr particji ustvarimo kratko tekstovno datoteko. Nato v disketno enoto računalnika znova vstavimo zagonsko disketo in prepišemo pravkar ustvarjeno sliko /usr particije nazaj na lokalni trdi disk. Potem znova poženemo računalnik z lokalnega trdega diska, se v operacijski sistem prijavimo kot administrator in pregledamo vsebino /usr particije. Če tekstovne datoteke na tej particiji ni več, smo lahko prepričani, da se je slika uspešno prenesla. Kasneje isti postopek ponovimo tudi s celotnim diskom [1, 3, 5, 6, 7].



Slika 19: Datoteke v mapi tftpboot.



Slika 20: Aplikacija za ustvarjanje slik oziroma pisanje slik na trdi disk.

4. ZAKLJUČEK

V pričujoči diplomski nalogi sem preizkusil programsko in strojno opremo, ki je namenjena zaščiti in obnavljanju vsebine trdega diska na javnih računalnikih. Ugotovil sem, da imajo tako varnostne kartice kot programska oprema Deep Freeze in Norton Ghost svoje prednosti oziroma slabosti.

Varnostne kartice so zaradi svojega načina delovanja skrite očem uporabnika, polega tega pa so izredno učinkovite in hitre pri obnavljanju vsebine trdega diska. Vsebina trdega diska je dosegljiva v trenutku, spremembe, ki jih na zaščiteni particiji napravi uporabnik, lahko s pravilno nastavitvijo delovanja varnostnih kartic ob vsakem ponovnem zagonu računalnika samodejno, brez posredovanja administratorja, pobrišemo. Torej se varnostne kartice v okolju, kjer je prisotnih veliko javnih računalnikov, odrežejo odlično. Slabost varnostnih kartic pa je v tem, da je za vsako novo namestitev programske opreme potreben precej zapleten in dolg postopek, s katerim dokončno namestimo programsko opremo. Slabost varnostnih kartic je tudi v tem, da je treba vsako kartico posebej nameščati v želen računalnik. Kartice so praviloma zelo drage in izredno krhke. Lahko se zgodi, da jo že ob vstavljanju v računalnik poškodujemo tako, da le-ta ne deluje več. Naslednja slabost varnostnih kartic je v tem, da se ob dodajanju točk obnove čas za nalaganje z določene točke obnove povečuje. Tako lahko uporabnik dobi občutek počasnosti nalaganja operacijskega sistema.

Uporaba programske opreme Deep Freeze ima skorajda enake značilnosti, kot uporaba varnostnih kartic. Tudi z uporabo programa Deep Freeze je namreč računalnik sposoben v trenutku obnoviti sliko trdega diska ali izbrane particije. Slabost v primerjavi z uporabo varnostnih kartic je v tem, da je programska oprema Deep Freeze sposobna obnavljati trdi disk samo iz ene točke in ne z večih, kot je to primer pri varnostnih karticah. Velika slabost uporabe programa Deep Freeze je tudi njegova tržna cena, ki je za različico Enterprise, ki dovoljuje namestitev na več javnih računalnikov, precej visoka. Se pa ta program odlično obnese pri delu na daljavo – tako je administrator sposoben nadzorovati celotno skupino javnih računalnikov s strežnika. Pri tem lahko izvede namestitev programske opreme Deep Freeze na več računalnikov hkrati in jim nastaviti potrebne parametre delovanja. Tako administratorju niti ni potrebno biti na mestu, kjer so javni računalniki, kar olajša in poenostavi njegovo delo.

Programska oprema Norton Ghost sicer ni sposobna obnoviti trdega diska v trenutku in na več računalnikih hkrati. Vendar je čas, ki je potreben za pisanje slike diska nazaj na računalnik, kratek. Tako lahko 40 GB trdi disk administrator obnovi tudi v dveh minutah, čas je odvisen od količine podatkov in programske opreme, nameščene na trdi disk. Pri uporabi te programske opreme ima administrator lahko za celo skupino strojno enakih računalnikov le en zagonski CD in eno sliko trdega diska. To poenostavi postopke in zmanjša prostor, ki je potreben za hranjenje slik trdega diska. Res pa je, da je ob hranjenju slik na strežniku potrebnega kar nekaj znanja in razumevanja delovanja programske opreme, da lahko sliko prepišemo nazaj na računalnik. To pa pomeni neprestano prisotnost administratorja.

Rešitev, ki sem jo izdelal, sem poskušal napraviti kar se da enostavno za uporabo. Posnema delovanje programske opreme Norton Ghost, kar pomeni, da tudi z uporabo te aplikacije ne moremo obnavljati trdega diska več računalnikov hkrati. Prav tako je čas prenosa slike trdega diska v sliko oziroma nazaj na trdi disk daljši kot pri programski opremi Norton Ghost, saj se v primeru moje aplikacije ustvari slika, ki je identična particiji ali celotnemu disku. Zato potrebujemo tudi več prostora na strežniku. Vendar, če je velikost particije dovolj majhna, se lahko čas, potreben za prenos, znatno zmanjša. Dobra stran moje aplikacije je tudi ta, da jo lahko uporablja vsak, ne samo administrator, saj je večina logike očem uporabnika skrita.

Uporabnik mora za pisanje nazaj na napravo poznati le ime datoteke, ki hrani sliko. Polega tega je ta aplikacija podobno kot programska oprema Norton Ghost uporabna tudi v primeru, ko je treba namestiti operacijski sistem in nabor programske opreme na več (na primer novih) računalnikov. Tako lahko prenesemo sliko trdega diska na vsak računalnik in se izognemo dolgotrajni namestitvi operacijskega sistema in programske opreme na vsak računalnik posebej. Dobra stran aplikacije pa je tudi v tem, da uporablja mrežni zagon. To pomeni, da bi lahko imeli na trdem disku javnega računalnika nameščen operacijski sistem Windows. Aplikacija bi brez težav lahko napravila sliko in jo zapisala nazaj na trdi disk, tudi če bi bil na tem disku operacijski sistem Windows. Res pa je, da se v tem primeru poraja vprašanje licenčnega operacijskega sistema, saj bi na vseh računalnikih obstajala kopija istega operacijskega sistema z isto registracijsko številko.

5. PRILOGE

Priloga 1: Seznam datotek v datoteki initrd.txt

```
/bin/
/bin/bash
/bin/obnovi
/bin/dd
/bin/gzip
/bin/mknod
/bin/mount
/bin/tftp
/dev/
/dev/console
/dev/null
/etc/
/etc/dhcpc/
/etc/hosts
/etc/nsswitch.conf
/etc/protocols
/etc/services
/lib/
/lib/3c59x.o
/lib/i686/
/lib/i686/libc-2.2.5.so
/lib/i686/libc.so.6
/lib/ld-2.2.5.so
/lib/ld-linux.so.2
/lib/libdl-2.2.5.so
/lib/libdl.so.2
/lib/libnss_files-2.2.5.so
/lib/libnss_files.so.2
/lib/libtercmap.so.2
/lib/libtermcap.so.2.0.8
/proc/
/sbin/
/sbin/dhcpcd
/sbin/insmod
/tmp/
/var/
/var/run/
```

Priloga 2: Bash skripta – obnovi

```
#!/bin/bash

export PATH=/sbin:/bin
```

```
tftp_server=192.168.1.11
mrezna=3c59x.o
naprava=hda
major_st=3
minor_st=( 0 2 )

mount -t proc proc /proc
insmod/lib/${mrezna}
/sbin/dhcpcd

while

meni="\n=============================================\n\n
        1.Prenesi image celotnega diska na streznik\n
        2.Prenesi image usr particije na streznik\n
        3.Zapisi image diska na napravo\n
        4.Zapisi image usr particije na napravo\n
        5.Izstopi iz aplikacije
        \n=============================================\n\n
\n Izberite moznost s pritiskom na stevilko:\c"

do
if [ ! -z „{ime}" ]; then \
        unset ime
fi

echo -e $meni
read ukaz
case $ukaz in

1)
        echo -e „Izberite ime za image datoteko:\t\c"
        read ime
                echo -e „\tImage se bo zapisal v datoteko:\t${ime}"
                ime_naprave=/dev/${naprava}${minor_st[0]}
                echo -e „\Izbrana naprava je:\t ${ime_naprave} (major_st, ${minor_st[0]})"
                echo -e „\Pricenjam s postopkom..."
                if [ ! -b ${ime_naprave} ]; then \
                        echo -e „Pricenjam z ustvarjanjem  slike ${ime_naprave}
                        mknod ${ime_naprave} b ${major_st} ${minor_st[0]}
                fi
                if [ ! -z „${ime}" ];  then \
                        if [ ! -p ${ime} ]; then \
                                echo „Ustvarjam cev"
                                mknod ${ime} p
                        fi
                fi
```

```
        tftp ${tftp_server} <<-EOT &
        binary
        put ${ime}
        EOT
        dd if=${ime_naprave}  |  gzip -c > ${ime}
        echo -e „Koncal sem s postopkom, pritisnite ENTER za ponoven pricetek“
        read p
        ;;
2)
    echo -e „Izberite ime za image datoteko:\t\c“
    read ime
        echo -e „\tImage se bo zapisal v datoteko:\t${ime}“
        ime_naprave=/dev/${naprava}${minor_st[0]}
        echo -e „\Izbrana particija je:\t ${ime_naprave} (major_st, ${minor_st[1]})
        echo -e „\Pricenjam s postopkom...“
        if [ ! -b ${ime_naprave} ]; then \
            echo -e „Pricenjam z ustvarjanjem  slike ${ime_naprave}
            mknod ${ime_naprave} b ${major_st} ${minor_st[1]}
        fi
        if [ ! -z „${ime}“ ];  then \
            if [ ! -p ${ime} ]; then \
                echo „Ustvarjam cev“
                mknod ${ime} p
            fi
        fi
        tftp ${tftp_server} <<-EOT &
        binary
        put ${ime}
        EOT
        dd if=${ime_naprave}  |  gzip -c > ${ime}
        echo -e „Koncal sem s postopkom, pritisnite ENTER za ponoven pricetek“
        read p
        ;;
3)
    echo -e „Izberite ime za image datoteko(datoteka mora obstajati na strezniku):\t\c“
    read ime
        ime_naprave=/dev/${naprava}${minor_st[0]}
        echo -e „\tIzbrali ste image datoteko:\t${ime}“
        echo -e „\Image se bo zapisal na:\t ${ime_naprave} (major_st, ${minor_st[0]})
        echo -e „\Pricenjam s postopkom...“
        if [ ! -b ${ime_naprave} ]; then \
            echo -e „Pricenjam z pisanjem na napravo ${ime_naprave}
            mknod ${ime_naprave} b ${major_st} ${minor_st[0]}
        fi
        if [ ! -z „${ime}“ ];  then \
            if [ ! -p ${ime} ]; then \
                echo „Ustvarjam cev“
```

```
                        mknod ${ime} p
                fi
        fi
        tftp ${tftp_server} <<-EOT &
        binary
        get ${ime}
        EOT
        gzip -c -d < ${ime} | dd of=${ime_naprave}
        echo -e „Koncal sem s postopkom, pritisnite ENTER za ponoven pricetek“
        read p
        ;;
4)
        echo -e „Izberite ime za image datoteko(datoteka mora obstajati na strezniku):\t\c“
        read ime
        ime_naprave=/dev/${naprava}${minor_st[1]}
        echo -e „\tIzbrali ste image datoteko:\t${ime}“
        echo -e „\Image se bo zapisal na particijo:\t ${ime_naprave} (major_st,
        ${minor_st[0]})
        echo -e „\Pricenjam s postopkom...“
        if [ ! -b ${ime_naprave} ]; then \
                echo -e „Pricenjam z pisanjem na particijo ${ime_naprave}
                mknod ${ime_naprave} b ${major_st} ${minor_st[0]}
        fi
        if [ ! -z „${ime}“ ]; then \
                if [ ! -p ${ime} ]; then \
                        echo „Ustvarjam cev“
                        mknod ${ime} p
                fi
        fi
        tftp ${tftp_server} <<-EOT &
        binary
        get ${ime}
        EOT
        gzip -c -d < ${ime} | dd of=${ime_naprave}
        echo -e „Koncal sem s postopkom, pritisnite ENTER za ponoven pricetek“
        read p
        ;;
5)
        exit;;

esac
done
```

Skripta ponudi uporabniku možnost ustvarjanja slik in pisanja teh datotek nazaj na trdi disk. Sestavljena je iz glavne zanke, ki ob vsakem prehodu najprej izniči vrednost spremenljivke ime. To sem dodal v skripto v primeru, če uporabnik večkrat zaporedoma požene izvajanje zanke. Lahko se namreč zgodi, da uporabnik želi pisati sliko celotnega diska v eno datoteko, nato pa še

sliko posamezne particije v drugo datoteko. Pri vsakem prehodu skozi zanko se vsebina spremenljivke počisti z namenom, da lahko uporabnik izbere novo ime za sliko. Pri vsakem prehodu skozi zanko mora uporabnik pritisniti številko, ki označuje izbiro. Nato se izvajanje skripte nadaljuje v enem od blokov znotraj izbire case. Tu skripta v primeru izbire ena ali dve od uporabnika zahteva, da vpiše ime datoteke, ki bo vsebovala sliko trdega diska ali /usr particije trdega diska. Zatem se ustvari naprava s stavkom mknod, ki mu je treba dodati stikalo b, ki pomeni block device, in glavno številko naprave ali številko particije, ki jo bo zapisal. Nato skripta preveri, če se je ustvarila cev, in jo ustvari, če ta še ni prisotna. Cev se ustvari z namenom, da lahko kasneje pišemo v datoteko na strežniku. Nato se na strežniku ustvari datoteka z imenom ${ime}, v katero se s programom dd v kombinaciji z ukazom gzip zapiše vsebina izbrane naprave. Zatem sledi obvestilo o končanem postopku. S pritiskom na tipko ENTER se uporabnik vrne v začetni meni.

V primeru pisanja na trdi disk ali /usr particijo je postopek isti, le da mora uporabnik poznati ime datoteke, v katerem je zapisana slika ali usr particije ali celotnega diska. V nasprotnem primeru lahko pride do napake, saj bi z zapiskom /usr particije na celoten trdi disk ali obratno lahko prišlo do nedelovanja računalnika. Postopek je nato povsem enak, le da se v primeru izbire tri in štiri s programom dd piše iz slike nazaj na napravo. Tudi v teh dveh primerih ob koncu zapisovanja na napravo sledi obvestilo o zaključku. S pritiskom na tipko ENTER se lahko uporabnik vrne na začetni meni. Izbira številke pet z začetnega menija pomeni izstop iz aplikacije.

6. REFERENČNA LITERATURA IN VIRI

[1] Clone script
Dostopno na: http://www.faqs.org/docs/Linux-HOWTO/Clone-HOWTO.html#CLONESCRIPT

[2] Disk cloning
Dostopno na: http://www.answers.com/topic/disk-cloning

[3] F. Jager, S.Divjak, Predloge za predavanja Sistemska programska oprema – Booting, 2005.

[4] Faraonics Deep Freeze User Guide
Dostopno na: http://www.faronics.com/doc/DF6Ent_Manual.pdf

[5] GNU GRUB
Dostopno na: http://www.gnu.org/software/grub/

[6] Kyle Rankin: PXE Magic: Flexible Network Booting with Menus
Dostopno na: http://www.linuxjournal.com/article/9963

[7] Linux home networking: Quick HOWTO: Ch 16: Telnet, TFTP and xinetd
Dostopno na:
http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch16_:_Telnet,_TFTP,_and_xinetd

[8] Neeta Garimella, TSM Client Developer, »Understanding and exploiting snapshot technology«
Dostopno na: http://www.ibm.com/developerworks/tivoli/library/t-snaptsm1/index.html

[9] Radix America LLC, Keeping the bussiness running
Dostopno na: http://www.radixamerica.com/howitworks.htm

[10] Radix Protector MLP, Quick User Guide
Dostopno na:
http://www.loidl-consulting.com/Portfolio/RADIX/RADIX_MLP_Quick_Guide_20-2-2003.pdf

[11] Symantec Norton Ghost User Guide
Dostopno na:
ftp://ftp.symantec.com/public/english_us_canada/products/ghost/14/manuals/ngh_14_user_guide.pdf

[12] What is disk imaging?
Dostopno na: http://www.tech-faq.com/disk-imaging.shtml