Digitalna forenzika mobilnih uređaja korišćenjem JTAG interfejsa

Predrag Alargić, Tanja Kaurin
Fakultet za pravne i poslovne studije dr Lazar Vrkatić
Novi Sad, Srbija
predrag.alargic@fpps.edu.rs, tanja.milosevic@useens.net

Sadržaj— **Digitalna forenzika je stalno suočena sa izazovom da zadrži korak sa najnovijim tehnologijama koje mogu biti upotrebljene u otkrivanju relevantnih tragova u okviru istrage. Problem digitalne forenzike mobilnih uređaja leži u tome što se različiti modeli u osnovi značajno razlikuju zbog stalnih izmena prouzrokovanih napretkom postojećih i brzim usvajanjem novih tehnologija. Ključ uspešne forenzičke analize leži u poznavanju hardvera i softvera uređaja koji je predmet istrage. U radu je dat detaljan prikaz pristupa podacima na mobilnom uređaju uz pomoć JTAG interfejsa radi ostvarenja komunikacije između računara i mobilnog uređaja baziranog na ARM platformi. Objašnjene su specifičnosti i prednosti JTAG interfejsa. Predstavljen je postupak analize podataka iz dobijenog fajla korišćenjem standardnih alata i programa i objašnjeno zašto se ovaj metod pristupa podacima smatra jednim od najsigurnijih.**

Ključne riječi - JTAG; digitalna forenzika; mobilni uređaj;

I. UVOD

Današnji mobilni uređaji predstavljaju spoj multifunkcionalnih i telekomunikacionih uređaja odnosno, jedinstveni spoj modernih tehnologija pristupačan svima kao neodvojivi deo svakodnevnice. Kao takvi, mobilni uređaji i tablet računari mogu da čuvaju veliku količinu podataka u sledećim formatima formatima :

- SMS poruke
- MMS poruke
- E-mail poruke
- Slike
- GPS lokacije
- GPRS, EDGE, 3G i WiFi pristupne tačke

Karakteristike i osobine samih uređaja postaju zanimljive kao nosioci informacija kako bezbednosnim strukturama radi prikupljanja dokaza, tako i kompanijama koje se bave izučavanjem sigurnosti podataka i sigurnosnim sistemima.

Mobilni uređaji predstavljaju dobar izvor dokaza i informacija sa stanovišta digitalnog dokaza. Osobenost analize na ovaj način prikupljenih dokaza i informacija se ističe u odnosu na forenziku računara koja je već u značajnoj meri standardizovana.

II. DIGITALNI DOKAZ

Prema međunarodnoj definiciji u oblasti forenzičkih nauka, digitalni dokaz je svaka informacija u digitalnom obliku koja ima dokazujuću vrednost, i koja je ili uskladištena ili prenesena u takvom obliku. Pojam digitalnog dokaza uključuje kompjuterski uskladištene i generisane dokazne informacije, digitalizovane audio i video dokazne signale, signale sa digitalnog mobilnog telefona, informacije sa digitalnih fax mašina i signale drugih digitalnih uređaja. Dakle, digitalni dokaz je bilo koja informacija generisana, obrađivana, uskladištena ili prenesena u digitalnom obliku na koju se sud može osloniti kao na merodavnu, tj. svaka binarna informacija, sastavljena od digitalnih 1 i 0, uskladištena ili prenesena u digitalnoj formi, kao i druge moguće kopije originalne digitalne informacije koje imaju dokazujuću vrednost i na koje se sud može osloniti, u kontekstu forenzičke akvizicije, analize i prezentacije.[1]

Digitalni dokazi imaju kako posredne tako i neposredne relacije prema krivičnom delu, a oni dobijeni na mobilnom uređaju, uz podatke dobijene posredstvom operatera mobilne telefonije mogu direktnije ukazivati na obavljene aktivnosti.

III. MOBILNI UREĐAJI KAO NOSIOCI INFORMACIJA

Mobilni uređaji se u osnovi sastoje iz standardnih komponenti kao što su : mikroprocesor, ROM (*eng. Read Only Memory*) memorija koja je nosilac operativnog sistema uređaja, RAM (*eng. Random Access Memory*) memorija koja je neophodna za rad radio modula, aplikacija itd. Skoro svi aparati rade na sličnom principu razlikujući se samo u hardverskim komponentama i karakteristikama. Svi oni podržavaju kako govornu tako i tekstualnu komunikaciju. Većina novijih uređaja poseduje i programe koji organizuju vaše obaveze i kontakte, a kao nosioci informacija su posebno interesantni sa aspekta digitalne forenzike.

Kada govorimo o softveru najnovijih uređaja, revoluciju su napravili pametni telefoni (smartphones) jer omogućavaju korišćenje velikog broja besplatnih programa. Omogućavaju pokretanje više programa istovremeno (multitasking) i kao takvi predstavljaju prave male računare, smeštene u minijaturno kućište.

Mobilni uređaji su i nosioci operativnih sistema, a na tržištu su se, između ostalih, posebno istakli "Android", "IOS" i "Microsoft" operativni sistemi.

Operativni sistemi omogućavaju instaliranje velikog broja aplikacija za komunkaciju koje ne koriste standardnu GSM mrežu, kao što su Skype, Viber i sl. Pored toga, omogućavaju korišćenje mesendžer programa za slanje i primanje kratkih poruka koji mogu da koriste i neke druge izvore internet saobraćaja kao što je WiFi i sl. Takav način komunikacije uveliko otežava prikupljanje potrebnih informacija, a često je i nemoguće prikupiti ih od GSM provajdera.

Digitalnu forenziku mobilnih uređaja možemo podeliti na dva segmenta, i to:

- forenziku memorije uređaja,
- forenziku SIM kartice.

U daljem radu bavićemo se isključivo forenzikom memorije mobilnih uređaja.

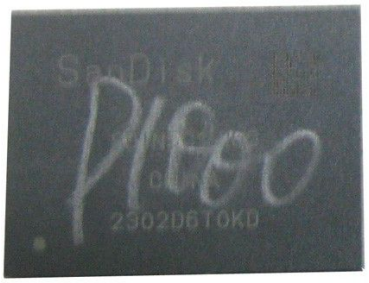
IV. FORENZIKA MEMORIJE UREĐAJA

Cilj forenzike memorije mobilnog uređaja je da se podaci koji su sačuvani u memoriji samog uređaja ekstrahuju i pronađu smisleni dokazi. Postoje dva pristupa podacima koja se nalaze u memoriji mobilnih uređaja [2].

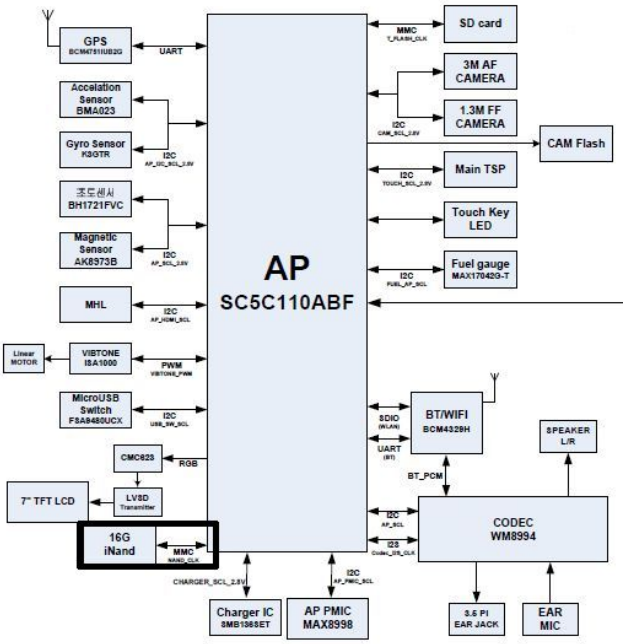
- Logički pristup - podacima koji se nalaze u memoriji se pristupa korišćenjem fajl sistema ili protokolom dobijenim od proizvođača samog memorijskog čipa.
- Fizički pristup - kompletan sadžaj memorije se iščitava uz pomoć nekog od uređaja bit-po-bit. Zatim se utvrđuje lokacija gde se nalazi potreban podatak.

U daljem radu pokazaćemo fizički pristup podacima u mobilnom uređaju uz pomoć JTAG (*eng. Joint Test-Action Group*) interfejsa [3].

U konkretnom slučaju u pitanju je tablet uređaj proizvođača Samsung koji nosi oznaku P1000. Uređaj poseduje NAND memoriju koja je zanimljiva za forenzičko ispitivanje zbog svoje složenosti (Sl. 1). Uređaji bazirani na NAND čipu takođe zahtevaju da u svojoj arhitekturi sadrže kontroler koji vodi računa o oštećenim blokovima. Kontroler može da bude u vidu drajvera ili zasebnog hardverskog uređaja (Sl. 2). U našem slučaju NAND memorija se oslanja na ECC (Samsungov algoritam) koji kontroliše rad i vodi računa o izgubljenim bitovima prilikom rada uređaja. Tipičan ECC može da ispravi grešku u jednom bit-u u svakom 2048-bitu (256 bajta) koristeći 22 bitni ECC kod. Kada korisnik obriše neki podatak iz NAND memorije uređaj može da detektuje blokove koji su "prividno" prazni i da ih označi, što znači da podaci nisu trajno obrisani, samo nisu trenutno vidljivi. Ova karakteristika NAND memorije nam može pomoći da lakše shvatimo strukturu samog čipa i način skladištenja podataka. Ovakva karakteristika NAND memorije je slična skladištenju podataka koji srećemo na tradicionalnim računarskim sistemima u obliku hard diska.



Slika 1. NAND memorija



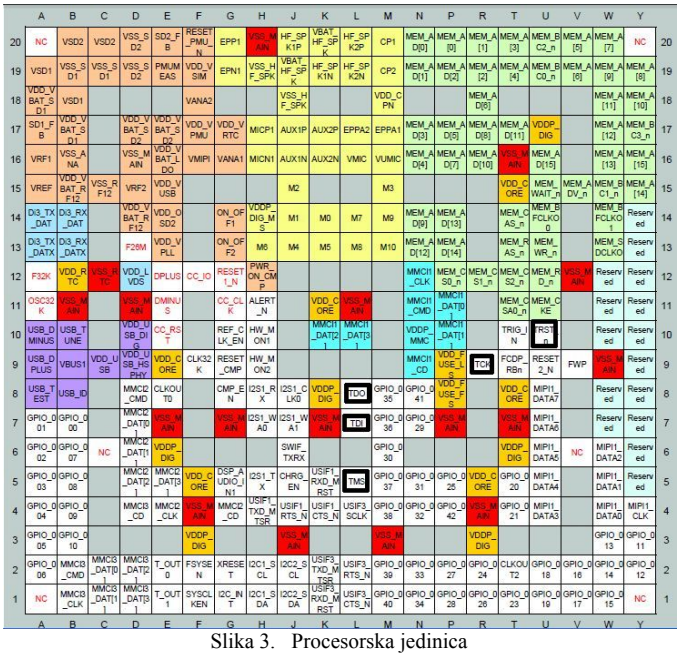
Slika 2. Arhitektura mobilnog uređaja

V. JTAG

Kada ne postoji niti jedan drugačiji način za forenzičko ispitivanje mobilnog uređaja, prelazi se na JTAG interfejs. JTAG kontakti na uređajima su prvenstveno namenjeni testiranju rada internog sofvera na uređajima, mada se mogu koristiti i da bi se pristupilo fleš memoriji uređaja. Iščitavanjem kompletnog sadržaja memorije preko JTAG interfejsa dobijamo kompletan forenzički dokazni materijal, koji u daljoj obradi možemo da analiziramo ili čuvamo za neku dalju obradu.

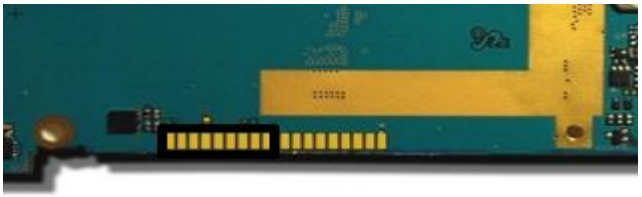
U ovom delu rada objasnićemo kako se nalaze test kontakti JTAG konekcije radi ostvarenja komunikacije između interfejsa i mobilnog uređaja, koji nisu lako dostupni krajnjim korisnicima.

Ako se prvi put srećemo sa modelom koji do sada nismo imali na forenzičkoj analizi problem može da predstavi lociranje potrebnih JTAG kontakata, koji po pravilu proizvođač sakriva na svojim uređajim. Pomoć zajednice forenzičara može u mnogome da skrati vreme pronalaženja JTAG kontakata, u slučaju da se neko već sretao sa istim modelom. Ako se prvi put srećemo sa modelom, moramo na samom uređaju da nađemo potrebne JTAG kontakte. Uz pomoć alata kao što je IRDA radna stanica, neophodno je skinuti procesorsku jedinicu i locirati potrebne signalne kontakte (Sl. 3). Signalni kontakti koji su nama bitni su : TMS, TRST, TDI, TCK, TDO, NRST i GND. Kada smo ih našli na nama pristupačnom mestu, procesorsku jedinicu uz pomoć IRDA radne stanice vraćamo na mesto i počinjemo sa postupkom uspostavljanja veze između JTAG interfejsa i mobilnog uređaja.



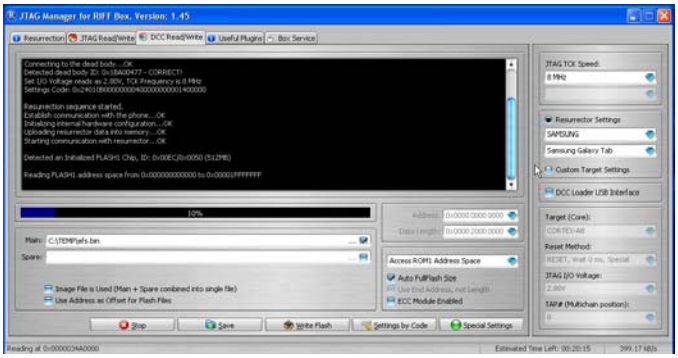
Slika 3. Procesorska jedinica

Na nekim modelima mobilnih uređaja JTAG kontakti su lako uočljivi i označeni. Međutim, postoje i modeli na kojima je proizvođač ostavio neoznačene JTAG kontakte (Sl. 4). Ipak, takvi modeli su retki, i sa pojavom novih modela mobilnih uređaja se sve ređe pojavljuju.



Slika 4. Neoznačeni JTAG kontakti

Povezivanjem mobilnog uređaja preko JTAG kontakata koje smo ranije pripremili i JTAG interfejsa (u našem slučaju se radi o univerzalnom JTAG interfejsu namenjenom otklanjanju neispravnosti na NAND memorijskim čipovima) ostvarili smo konekciju sa mobilnim uređajem (Sl. 5).



Slika 5. Povezivanje i čitanje sadržaja NAND memorije

Da bi ostvarili komunikaciju između NAND memorije i JTAG uređaja, koristili smo DCC kanal (*eng. Data Communication Channel*) koji je dostupan skoro u svim NAND memorijama. Selektovanjem odgovarajuće adresne veličine loader vrši komunikaciju direktno sa memorijskim kontrolerom kako bi omogućio pristup sadržaju memorijskog čipa. DCC loader uspostavlja komunikaciju između interfejsa i programskog koda unutar memorijskog čipa. Informacije između JTAG interfejsa i memorijskog čipa prolaze kroz DCC kanal koji je dostupan u skoro svim ARM (*eng. Advanced RISC Machines*) procesorskim jezgrima (ARM procesori su bilo koji 32-bitni RISC, *eng. Reduced Instruction Set Computer*, mikroprocessori napravljeni od strane Advanced RISC Machines, Ltd). To znači da nije važno koji hardverski uređaj imamo ispred sebe, bio to mobilni telefon ili tablet računar, nezavisno od proizvođača ili karakteristika istog, važno je samo da znamo koje je veličine NAND memorija. Kada imamo tu informaciju dovoljno je samo da odaberemo adekvatan DCC loader i uz pomoć istog pristupamo NAND memoriji uređaja [4].

Da bi pročitali neki izraz (32 bita) iz Debagera (*eng. Debugger*) JTAG interfejsa, kod koji se pokreće unutar DCC loadera treba da izvrši sledeću instrukciju unutar ARM procesora :

MRC p14, 0, Rd, c1, c0, 0

koja premešta izraz u Rd registar. Da bi poslali izraz u debager, DCC loader treba da izvrši sledeću instrukciju :

MCR p14, 0, Rd, c1, c0, 0

koja pokreće izraz iz Rd registra u DCC kanal i zatim smešta u debager (JTAG interfejs).

Svaki DCC paket koji je primljen od loadera ima sledeću strukturu :

```
{
unsigned int dLength;
unsigned int dData[dLength];
unsigned int Checksum;
  } DCC_Packet;
```

Prva reč je dLength - kvantitativni izraz, koji je praćen specifičnim brojem podataka i na kraju čeksum izraz, koji je ustvari CRC32 čeksum (*eng. Cyclic Redundancy Check*).

Na početku , DCC loader šalje pakete primaocu koje sadrže dve reči :

Word1, Word2

To je potrebno da bi DCC loader postavio donju polovinu od *Word1* u vrednost 0x4B4F a softver koji kontroliše komunikaciju znao da je DCC loader startovao dobro. Gornja polovina *Word1* je NAND page veličine u bajtovima

```
PageSize = Word1 >> 0x10
```

Nakon uspešno ostvarene konekcije između mobilnog uređaja i JTAG interfejsa i iščitanog sadržaja potrebno je dobijene podatke prevesti u nama razumljive, odnosno podatke koji se mogu iskoristiti kao dokaz.

Kada je memorija uspešno preuzeta sa telefona neophodna je njena detaljna analiza. Informacije koje su nama bitne se ne nalaze u obliku koji je nama potreban. U ovom odeljku se razmatraju metode koje se koriste i koje potpuno rekonstruišu forenzički relevatan sadržaj. Korisnički podaci koji se dobiju i analiziraju iz iščitane memorije mobilnog uređaja tada dobijaju nama zadovoljavajući oblik.

Svi postojeći alati koji bi mogli da analiziraju "Linux memory dumps", odnosno koji mogu da prevedu iščitani sadržaj su fokusirani na Intel arhitekturu zbog njene popularnosti. Veoma je bitno razumeti da je ARM arhitektura koja se pokazala kao vodeća u mobilnom svetu postaje sve više neophodna forenzičkim istražiteljima. Sa aspekta forenzike iščitanog sadržaja osnovna funkcija za podršku ARM arhitekture je sposobnost prevođenja iz kodiranog sadržaja u nama fizički prepoznatljiv oblik.

U ovom radu smo koristili alat pod nazivom X-way forensic [5], radi analize iščitanog sadržaja ali isto tako i radi provere samog sadržaja. Pored već pomenutog softverskog alata korišćene su skripte pisane u Python [6] programskom jeziku. Napravljene skripte nam služe da iz iščitanog sadržaja NAND memorije korišćenjem JTAG interfejsa, a nakon analize i određivanja lokacije uz pomoć X-way forensic programa, dobijeni sadržaj prevedemo u nama razumljiv i validan dokaz.

Prvi korak je da izračunamo MD5 i SHA1 čeksum iz iščitanog sadržaja, odnosno iz dela sadržaja koji želimo da analiziramo. Ovaj korak je i najbitniji jer se njime garantuje integritet podataka. U sledećem koraku deo sadržaja nad kojim vršimo forenzičku analizu razdvajamo na nekoliko sekcija (Sl. 6). Pojedinačni blokovi u okviru sekcije se izoluju čime se olakšava dalji proces analize. Nakon što su blokovi razdvojeni za forenzičku analizu, biramo blok koji treba da se analizira. U konkretnom slučaju je pokazano kako da se izdvoji imenik sa nama važnim podacima iz izolovanog bloka.

```
----> starting script.....

----> opening file : ecs.bin

----> Samsung android

----> generating hash values.....
md5 value :  d3eacc3erg554f89h43b73a4e22b76
sha value :  0075e55h7aac13bb21d0d859c8e27dd327g882a4
----> end hash values....
----> creating output folder : Samsung android/cuttedPieces_HEX/
----> creating output folder : Samsung android/cuttedPieces_ASCII/
----> creating output folder : Samsung android/media/
----> creating output folder : Samsung android/XML/

----> IMEI : XXXXXXXXXXXXXXX
```

Slika 6. Skripta

Kada smo sve ovo pomenuto uradili, korišćenjem skripte uveli smo podatke u Microsoft Excell tabelu. Tako dobijeni podaci dovedeni su u oblik koje je prihvatljiv kao forenzički dokaz (Sl. 7).

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:element name="contact">
    <xsd:annotation>
      <xsd:documentation>Saved contacts</xsd:documentation>
    </xsd:annotation>
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="id"              type="xsd:int"/>
        <xsd:element name="number"          type="xsd:string"
            minOccurs="0" maxOccurs="unbounded"/>
        <xsd:element name="name"            type="xsd:string"/>
        <xsd:element name="email"           type="xsd:string"
            minOccurs="0"/>
        <xsd:element name="url"             type="xsd:string"
            minOccurs="0"/>
        <xsd:element name="address"         type="xsd:string"
            minOccurs="0" maxOccurs="unbounded"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
</xsd:schema>
```

Slika 7. XML-schema za snimljene kontakte

VI. ZAKLJUČAK

Forenzičari digitalnih medija i mobilnih tehnologija se konstantno suočavaju sa novim izazovima, problemima i stalnim napretkom tehnologije. To iziskuje konstantno učenje i snalaženje u novonastalim situacijama vezanim za spoznaju najnovijih tehnologija koje se upotrebljavaju radi razotkrivanja relevantnih tragova u istrazi. Ceo dinamični sistem koji uključuje proizvođače telefona i tablet uređaja, proizvođače forenzičkog alata, izvršioce krivičnih dela i forenzičare, kao i organe gonjenja čini ovu delatnost još složenijom.

Konstantnim unapređenjem svojih proizvoda, proizvođači mobilnih tehnologija često menjaju operativne sisteme, sisteme datoteka i tako otežavaju posao forenzičarima. S obzirom da su dokazi dobijeni prikupljanjem digitalnog materijala sve zastupljeniji u krivičnom postupku i da je njihov značaj veliki, problemi koji mogu da nastanu moraju se prevazići primenom kvalitetnog alata i izborom odgovarajućeg pristupa i metoda za svaki slučaj ponaosob.

Prikupljanje forenzičkog materijala, odnosno dokaza preko JTAG interfejsa, na način objašnjen u ovom radu je metod koji se primenjuje samo u određenim slučajevima. Razlog primene

ovog metoda je kada uređaj na kojem želimo da izvršimo forenzičku analizu nije potpuno ispravan ili je neispravan u pogledu standardne komunikacije. Na ovaj način dobijamo kompletnu sliku, odnosno kompletan sadžaj celokupne memorije. Korist od primene ove metode se ogleda i u mogućnosti povrata podataka koje je korisnik izbrisao iz uređaja (SMS poruke, imenik i slično) jer je jedini način da ih povratimo iz memorije - iščitavanjem NAND memorije. Budućnost ovog principa sakupljanja forenzičkih podataka je u usavršavanju analize iščitanih podataka analizirajući FTL (*eng. Flash Translation Layer*).

LITERATURA

[1] L. Petrović, "Digitalni dokazi", ZITEH '04, Jun 2004.

[2] K. Kim, D. Hong, K. Chung, J. Ryou, "Data acquisition from cell phone using logical approach", World Academy of Science, Engineering and Technology 8, 2007.

[3] http://www.amontec.com/pub/amt_ann004.pdf

[4] Rocker team , "RIFF Box JTAG™ User manual", 2010.

[5] http://www.x-ways.net/forensics/, pristupljeno Januar 2013.

[6] M. Lutz, "Programming Python", O'Reilly, Septembar 2001.

ABSTRACT

Digital forensic community is under a lot of pressure to remain on a par with the latest technologies that may be utilized in order to expose relevant investigation clues. The mobile devices digital forensics problem is that they significantly vary in design as they are being subjected to constant changes as existing technologies improve and the new ones are being introduced. The key to successful forensic analysis stems on a knowledge of investigated device's both hardware and software platforms. The present paper provides a detailed data access account to mobile device utilizing JTAG interface for establishing communication between computers and mobile devices based on the ARM platform. Explained are the JTAG interface characteristics and advantages. Presented is the data analysis procedure from the resulting file utilizing the standard tools and software and explained reasons for this data access method to be considered one of the safest.

DIGITAL FORENSICS OF MOBILE DEVICES UTILISING JTAG INTERFACE

Predrag Alargić
Tanja Kaurin