ЗБОРНИК НА ТРУДОВИ

Петта меѓународна научна конференција
„ Науката - подршка на развојот во Југоисточна Европа “

Скопје 15-16 декември 2017

ЗБОРНИК НА ТРУДОВИ: Петта меѓународна научна конференција
„Науката – подршка на развојот во Југоисточна Европа“

Организатор: Институт за дигитална форензика
Универзитет „Евро-Балкан“ - Скопје

Уредник: Проф.д-р Сашо Гелев

Издавач: Универзитет „ЕВРО-БАЛКАН“ Скопје
Република Македонија
www.euba.edu.mk

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

001.3:330/378(497.7)(062)

МЕЃУНАРОДНА научна конференција (5 ; 2017 ; Скопје)
Науката - поддршка на развојот во Република Македонија : зборник
на трудови /Петта меѓународна научна конференција, Скопје 15-16 декември, 2017 ;
[уредник Сашо Гелев]. - Скопје: Универзитет
"Евро-Балкан", 2017. - 145 стр. : илустр. ; 30 см

Текст на мак. и англ. јазик. - Фусноти кон текстот. - Библиографија кон трудовите

ISBN 978-608-4714-19-4

а) Научен развиток - Општествени науки - Македонија - Собири
COBISS.MK-ID 105396490

Програмски одбор

- **Проф. Д-р Драгор Заревски, Универзитет Евро Балкан – Претседател;**
- **Проф. Д-р Сашо Гелев – Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија копретседател;**
- **Проф. д-р Влатко Чингоски, Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија;**
- **Проф. Д-р Божо Крстајиќ, Електротехнички факултет - Подгорица, Црна Гора;**
- **Проф. Гоце Митревски, Аубурн Универзитет, Аубурн, САД;**
- **Проф. Денис Химчи, Универзитет „Александар Џувани“, Елбасан, Албанија;**
- **Проф. Ахмед Ајтач, Селџук Универзитет,Конија, Турција;**
- **Проф. Кубилај Акман, Ушак Универзитет, Ушак, Турција;**
- **Проф. Светлана Антова, Бугарска Акаемија на Науките, СОфија, Бугарија;**
- **Проф. д-р Здравко Скакавац, Факултет за правне и пословне студије, Универзитет УССЕ, Нови Сад;**
- **Проф. д-р Лада Садиковиќ, Факултет за криминалистика, криминологија и безбедност, Универзитет во Сараево;**
- **Проф. д-р Гордан Калајџиев, Правен факултет, Универзитет Св. Кирил и Методиј – Скопје, Република Македонија;**
- **Проф. Д-р Никола Протрка, Полициска академија, Загреб, Република Хрватска;**
- **Проф. Д-р Стефан Сименов, Академија за внатрешни работи на Република Бугарија;**
- **Доц. д-р Снежана Черепналковска Дуковска, Универзитет Евро Балкан, Република Македонија, член**
- **Доц. д-р Мимоза Клековска, Универзитет Евро Балкан, Република Македонија, член;**
- **Проф. д-р Роман Голубовски, Природно математички факултет,Универзитет Св. Кирол и Методиј Скопје, Република Македонија;**
- **Проф. д-р Марјан Николовски, Факултет за безбедност, Универзитет Св. Климент Охридски, Битола, Република Македонија.**

Организациски одбор

- **Проф. д-р Сашо Гелев, – Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија, претседател;**
- **Доц. д-р Мимоза Клекоска, Универзитет Евро Балкан, Република Македонија, член;**
- **Проф. Д-р Божо Крстајиќ, Електротехнички факултет - Подгорица, Црна Гора, член;**
- **Доц. д-р Снежана Черепналковска Дуковска, Универзитет Евро Балкан, Република Македонија, член;**
- **Проф. Гоце Митревски, Аубурн Универзитет, Аубурн, САД, член;**
- **Проф. Денис Химчи, Универзитет „Александар Џувани“, Елбасан, Албанија, член;**
- **Проф. Ахмед Ајтач, Селџук Универзитет,Конија, Турција, член;**
- **Проф. Кубилај Акман, Ушак Универзитет, Ушак, Турција, член;**
- **м-р Игор Панев, Универзитет Евро Балкан, Република Македонија, член;**
- **Зорица Каевиќ, Универзитет Евро Балкан, Република Македонија, член;**
- **Ивана Гелева Универзитет Евро Балкан, Република Македонија, член.**

П Р Е Д Г О В О Р

Позади нас е уште една конференција „Науката-подршка на развојот во Југоисточна Европа одржана од 15 до 16 декември 2017 година во Скопје, а ова е зборникот на трудови кои се презентирани на конференцијата. Програмскиот одбор и реценентскиот тим изврши селекција и овде се презентирани само прифатените трудови.

Пред пет години за прв пат ја организиравме оваа конференција со цел студентите од вториот и третиот циклус на студии да се оспособат за пишување и презентирање научно-стручни трудови, а останатите учесници да ги пренесат своите најнови истражувања во посочените области.

Пред Вас се 19 квалитетни трудови презентирани во 4 секции.

Организаторот се надева дека и присутните го делат ова мислење дека ова е една од поуспешните конференции. Ова не обврзува и следните конференции да бидат со ист квалитет, нови луѓе, нови теми, нови акции и ист дух на конференцијата.

Проф. Д-р Сашо Гелев

СОДРЖИНА

Иван Петров

Универзитет Евро Балкан Скопје

Република Македонија

Сашо Гелев

Електротехнички Факултет,

Универзитет Гоце Делчев- Штип, Македонија

ПРЕПОРАКИ ПРИ ПРОЕКТИРАЊЕ НА ЛАБАРАТОРИЈА ЗА ДИГИТАЛНА ФОРЕНЗИКА

Апстракт: *Брзо растечките стапки на комјутерски криминал во последните години ја зголемува потрбата од квалитетни истаги за дигитален кримиал, а со тоа и изгрдба на акредитирана лабараторија за дигитална форензика која ке може да одговори на поставените задачи од стрна на соодветните институции.*
Во овој труд ќе се обидеме да ги дадеме препораките кои треба да се следат при проектирање на лабараторија за дигитална форензика. Лабарарторијата која е направена врз база на овие препораки многу лесно ќе биде акредитирана од страна на соодветните институции.

Клучни зборови*: Дигитална форензика, Лабараторија за дигитална форензика.*

RECOMMENDATIONS FOR PROJECTING A LABORATORY FOR DIGITAL FORENZIC

Abstract: *Rapidly rising rates of computer crime in recent years have increased the demand for high-quality digital crime investigations, and thus the construction of an accredited laboratory for digital forensics that will be able to respond to the requirements set by the appropriate institutions.*
In this labor we will try to give the recommendations that should be followed when designing a laboratory for digital forensics. The laboratory, which is based on these recommendations, will be very easily accredited by the appropriate institutions.

Key words: *Digital Forensics, Digital Forensic Laboratory.*

1. ВОВЕД

Во 2011 година, Internet Crime Complaint Center (IC3) активно се занимава со злосторства извршени преку Интернет, обезбедувајки услуги за жртвите на онлајн злосторства и за Јавните обвинителства. Во извештајот на IC3 се наведува дека IC3 добил повеќе од 300.000 претставки, односно зголемување од 3,4% во однос на претходната година [1]. А со тоа и вкупна загуба од 485,3 милиони долари.

Покрај тоа, The Federal Bureau of Investigation’s (FBI) Regional Computer Forensics Laboratory (RCFL) откри дека бројот истражители кој вршат истраги во полето на компјутерскиот криминал бил 7629. Односно, (RCFL) извшиле обработка на 4263 TB на податоци во 2011 година[2].

Видовите на компјутерски криминал се бројни, а најчести се следните:

- Крадење на компјутерските сервиси,
- Неовластен пристап,

- Пиратерија со софтвер,
- Откривање, крадење и промена на компјутерските податоци и информации,
- Изнудување со помош на компјутер,
- Неовластен пристап до базите на податоци,
- Злоупотреба на украдена лозинка,
- Пренос на деструктивни вируси и
- Индустриска и политичка шпијунажа.

Дигитална форензика е збирка на
специјализирани техники, процеси и процедури кои се користат за :

- чување,
- собирање,
- валидирање,
- идентификација,
- анализа,
- интерпретација,
- документирање и
- презентација на дигиталните докази од различни извори [3].

Без оглед на случајот, секој кој сака да работи во полето на дигиталната форензика мора прво да ги научи основните техники, процеси и процедури за да успее. Но за да успехот биде гаранитран и поткрепен со бројни докази истражителот односно дигиталниот форензичар треба да работи во соодветно изградена лабараторија која ги содржи основните елементи за напречено функционирање кој ке бидат разгледани во овој труд.

2. Препораки од полето на физичкиот изглед на лабараторијата за дигитана форензика

2.1.Електрична инсталација

Поставувањето на соодветната електрична инфраструктура може да ја одржи чувствителната опрема од тековните падови на напонот на електричната струја. При самото проектирање треба да го земе предвид видот на опремата, вкупната потрошувачка, можните падови на напон при стартување на уредите како и можностите за понатамошно надоградување на уредите односно и на самата лабараторија.

За разлика од другите апарати, компјутерите користат осцилирачко напојување кое при самата работа може да создаде ефект на хармониски осцилаци. Горе наведенето задно со промената на напонот може да предизвика трајно оштетување кај транзисторите и отопорниците на поставените уреди

При проектирањето на електричната инсталација треба да се земат впредвит следните препораки :

- Да не се поврзуваат повеке од два компјутера на еден осигурувач и истите да не се комбинираат во струјното коло со други уреди како што се печатачи, копири и скенери.
- Секој компјутер да биде посебно приклучен на (UPS) систем.
- Да се постави соодветно заземјување и громобранска заштита.[4]

2.2.Греење, вентилација и климатизација (HVAC)

(HVAC) можат да бидат дизајнирани слично на оние во канцеларијата со систем за ниско-брзински воздух, што резултира со значителни заштеди на енергија. Но секогаш во

предвид треба да се зема максималното топлинско оптоварување од постоваената опрема и бројот на луѓе кои ке работат во лабараторијата. [4]

2.3.Акустика

Акустиката на лабораторијата и околните површини се важни за дизајнот поради чуствителноста на работа. Едноставно кажано, лабораторијата треба да биде колку што е можно подобро звучно изолирана. Секоја дискусија на истражителите кои ги имаат деталите за случаите може да ја нарушат тајноста на предистражната постапка, да ја повредат приватност на инволвираните лица или исите да бидат навредливи ако се слушнат од страна на персоналот надвор од лабораторијата.

При проектирањето на акустичната изолација треба да се земат впредвит следните насоки :

- Поставување на теписи. Подните облоги ја апсорбираат бучават и паршината во самата просторија
- Да се постават плочки или апсорбери на звук на таванот
- Поставување на извор на бучава во лабораторијата. Ова може да биде толку едноставно како што е поставување на радиото или да се користи извор на бел шум.
- Додавање на звучна изолација на периметарските ѕидови како дополнителна мерка на приватност.
- Да се постави антистатичен под на целата површина од лабараторијата со тоа што освен добар звучен изолатор истиот може да се користи и за спроведување на електричната и мрежната инсталација до самите уреди. [4]

2.4.Работен простор

Големината и изгледот на лабораторијата ќе влијаат на нејзината продуктивност. Основен изгледот лабораторијата треба да содржи работен простор за секој истражител и заеднички простор за складирање и евидентирање на работните материјали.

При проектирањето на работниот простор треба да се земат впредвит следните насоки:

- Минималната површина за секоја испитувачка станица треба да биде 5 квадратни метри. Препорачаната површина за секоја испитувачка станица е 7 квадратни метри.
- Секој работен простор има потреба од работна маса кој треба биде минимум 130 см долга и 90 см широка а при самиот избор на истата траба да се земе впредвид поставување на печатар и други периферни уреди.
- Сефовите се одлични за складирање на хард дискови и други мали периферни уреди. Доколку станува збор за чување на материјали на кој се наоѓаат класифицирани информаци препорачливо е набавка на сефови со безбедносна категорија три(3).
- Фиокарите за докази се одлични за складирање на хард дискови и други медиуми додека се обработуваат.
- Осведлувањето на просторијата треба да биде на завидно ниво.
- Компијутерските монитори треба да бидат поставени во спротивен правец од прозорците за да немаме проблем со надворешната светлина.

За време на компјутерска форензичка истрага, истражителот може да седи пред компјутеркиот екран осум или повеќе часови дневно. При проектирањето на работниот простор треба да се земат впредвит следните насоки:

- Столот треба да им овозможи на истражителите да ја прилагодат висината на седиштето и наваленоста
- Столовите треба да имаат потпирачи за раце кои можат да се прилагодат на висината.
- Мониторите треба да бидат поставени директно пред испитувачот и да бидат прилагодливи за да се намали оптоварувањето на вратот и очите. [4]

2.5.Безбедност

При процесирање на дигитални докази секогаш треба да се земе во обзир тајноста на самата постапка а со тоа и зачувување на приватноста на лицата односно самата пресункција на невиност. Најдобро при проектирањето на лабараторијата истата да биде во согласност со законот за класифицирани информаци односно со уредбите за :

- Административна безбедност
- Безбедност на лица
- Физичка безбедност
- Индустриска безбедност
- Информатичка безбедност

А самите процедури кои ке се користат во лабароторијата да бидат во согласност со ISO/IEC 27037 : 2013 [5]

3. Препораки за набавка на соодветен хардвер и софтвер

3.1 Хардвер

3.1.1. FRED работната станица

Едно од најдобрите хардверски решенија кое се нуди денеска на пазарот е FRED работната станица.

FRED работната станица е оптимизирана за работа во стационарни лабараториски услови но исто така може да се набави и FRED работна станица за теренска истрага. Истата се одликува со брза обработка на осомничените тврди дискови односно аквизација на податоците од. IDE/EIDE/ATA/SATA/ATAPI/SAS/Firewire/ USB тврди дискови. Како и уреди за складирање на податоци од типот Blu-Ray, DVD, CD Compact Flash, Micro Drives, Smart Media, Memory Stick, Memory Stick Pro, xD Cards, Secure Digital Media и Multimedia Cards. FRED работната станица вклучува UltraBay, надворешен панел каде што може да се врши лесна замена на тврдите дискови каде што истражителот ги складира аквизираните дигитални докази.

Стандардната FRED работна станица поседува три high speed drives (два SSDs и еден 7200rpm HDD). Првиот SSD се користи за инсталација на оперативниот систем и форензичките алатки вториот SSD складирање и инсталација на Temp/Cache/DataBase. Додека на третиот диск се складираат и обработуваат аквизираните дигитални докази.

Преостанати хардверски карактериситки на стандардната FRED работна станица се :

- 23 3/4" High, 8 3/8" Wide, 25 1/4" Deep - 80 lbs
- Intel Core i7-6800K CPU (Hex Core Processor), 3.4 GHz, 15MB Intel Smart Cache
- 32 GB (2x16GB)PC3-17000 DDR4 2133 MHz Memory
- 1 x 256 GB Solid State SATA III Drive - OS Drive
- 1 x 256 GB Solid State SATA III Drive - Temp/Cache/DB Drive
- 1 x 2.0 TB 7200 RPM SATA III Hard Drive - Data Drive installed in HotSwap Bay1
- Nvidia GTX 1050Ti 4GB 128 bit DDR5 PCI-Express Video Card with 1 DisplayPort, 1 HDMI, and 1 DVI-D Ports
- 22" WideScreen LCD Monitor with Built-in Speakers

FRED работна станица ги има интегрирано следните физички Write Blocker

- Интегриран IDE Drive Write Blocker
- Интегриран SATA Drive Write Blocker

- Интегриран SAS Drive Write Blocker
- Интегриран USB 3.0/2.0 Write Blocker
- Интегриран FireWire IEEE 1394b Write Blocker
- Интегриран PCIe Write Blocker

FRED работна станица подржува инсталација на двата најпознати софтверски решенија за анализа на дигитални докази [6]

- AccessData FTK и
- EnCase

3.1.2. Хардверски препораки при креирање работна станица

Во случај институција да не е во можност да набави специјализирана работна станица при креирање на истата треба да набави најдобри хардверски решенија кои се нудат на пазарот со цел да обезбеди максимална брзина на аквизација и анализа на дигитлните докази.

Посебно кога се врши креирање на работната станица треба да се внимава на изборот на физички Write Blockers

Физичките Write blockers се уреди кои овозможуваат аквизација и верификација на дигиталните докази без притоа да се изврши оштетување на или запишување на податоци на осомниченият носач на податоци. Нај барани во моментот на пазарот се :

- Tableau
- UltraKit III
- WiebeTech
- Logicube
- ICS Drive Lock

Освен физичките може да се користат и логички Write Blocker’s и истите можат да се набаваат како софтверски решенија во зависност од оперативниот систем. [7]

3.1.3. Избор на тврди дискови за складирање на аквизираните дигиралн докази

За складирање на аквизираните дигитални докази потребно е да имаме соодветни тврди дикови а нивниот избор се врши во зависност од мемориската зафатнина на дигиталниот доказ (500 GB , 1 TB, 2 TB), конекцијата на самиот тврд диск со работната станица (min SATA III), брзината на конекцијата. Во случај на хитна постапка можат да се користат и SSD дискови[7].

3.1.4. Останати потребни периферни елементи

За непречено функционирање на лабараторијата потребни се следните периферни елементи :

- Кабли за електрично напојување
- Искористени тврди дискови
- Рачен алат за демонтажа и монтажа на хардверски елементи
- Анти статични душеци за пакување и складирање на прибавените докази
- Кабли, конектори и адаптери

Еден 8" IDE Interface Cable

Еден 2" IDE Interface Cable
Еден SATA Interface Cable
Еден SCSI-3 Interface Cable
Еден 1.8" Hard Drive Adapter
Еден 5" Hard Drive Adapter
Еден One ZIF Hard Drive Adapter
Еден MicroSATA Adapter
Еден eSATA to eSATA Cable
Два USB A to Mini 5 pin Cables
Еден FireWire A (6 pin - 6 pin) Cable
Два FireWire B (9 pin - 9 pin) Cables
Еден FireWire A (4 pin - 9 pin) Adapter
Еден FireWire A (6 pin - 9 pin) Adapter
Комплетен сет од конектори за мобилни телефони.

3.2.Софтвер

Следните повекенаменски дигитално форензички софтвери доаѓаат од водечки компании во оваа поле и ги покриваат речиси сите аспекти на една современа форензичка истрака од процесот на аквизација, анализа и крерање на завршни репорти за употреба пред надлежните институции.

Водечки компании во оваа поле се :

- EnCase From Guidance Software и
- FTK From AccessData

И двата софтверски пакети се признаени од судската власт во САД и препорака е да се набават и двата со цел при комплексна истрага доказите да бидат потврдени од страна да двете софтверски решенија.

Освен овие софтверссски решенија со затворен код на пазарот можат да се најдат уште многу софтверски решенија со затворен и со отворен код [8][9]

3.3.Софтвери за форензика на мобилни уреди

На пазарот се нудат исто така и голем број на софтверски решенија за дигитална форензика на мобилни телефони и други уреди кои ја користат мобилната мрежа, GPS мрежата, дронови и други мали уреди.

Водечки компании во оваа поле се :

- XRY [10]
- Oxygen Forensic
- Cellebrite
- Paraben's Mobile Field Kit

При самиот избор на софтвер за форензика на мобилни уреди треба да се земе впредвит бројот на уреди односно модели кај кои може да се изврши комплетна дигитално форензичка анализа.

4. Заклучок

Врз онова на горенаведеното можеме да заклучиме дека има голем број на детали кои треба да се земат при проектирање на лабараторија за дигитална форензика.

Од физички аспект акцентот треба да се стави најмногу на безбедноста на дигиталните докази како за времето на нивно процесирање и чувањето на истите со цел да не дојде до нивно оштетување а со тоа и одбивање како дел од доказниот материјал од страна на надлежните институции. Исто така од физички аспект треба доста да се внимава на обезбедување на солидни работни услови на истражителите. Бидејќи процесирањето на дигиталните докази може да трае и со денови.

Хардверот и софтверот кој ке се избере за обработка на дигиталните докази треба да биде прифатлив од судската власт.

Од хардверски аспект лабараторијата треба да ги поседува сите неопходни алатки за да може да се изврши аквизација на дигиталните докози вклучувајќи алат за демонтажа сет на кабли, конектори и адаптере за да се изврши неопходното поврзување на прибавените носачи на меморија со работните станици. Исто така треба да се внимава и константо да се извршува тестирање на физичките и логичките Write blockers со цел да не дојде до запишување на податоци од работната станица кон дигиталниот доказ.

Од софтверски аспект треба да поседуваме што е можно повеке апликации за анализа на дигиталните докази а со самото тоа да можеме да извршиме и проверка на сработеното пред истото да се презентира пред надлежните институци.

Користена литература

[1] IC3 2011 Internet Crime Report, http://www.ic3.gov/media/2012/120511.aspx

[2] Regional Computer Forensics Laboratory Annual Report for FY 2011, http://www.rcfl.gov/downloads/documents/FY11_annual_report_web/annual_01-1_intro.html.

[3] Дигитални Докази – Електронски криминал д-р Ристо Христов.

[4] Digital Forensics: Architectural and Engineering Facility Design Requirements by Michael MountAdam Denmark

[5] Закон за класифицирани информации (Св. на РМ бр.9 од 27.02.2004)

[6] https://www.digitalintelligence.com/products/fred/

[7] Wen Yao, Chao-Hsien Chu, Bing Liu and Zang Li: Designing a virtual lab for computer forensics. In Proc. of the 14th Colloquium for Information Systems Security Education, Maryland (2010).

[8] https://accessdata.com/products-services/forensic-toolkit-ftk/

[9] https://www.guidancesoftware.com/

[10] https://www.msab.com