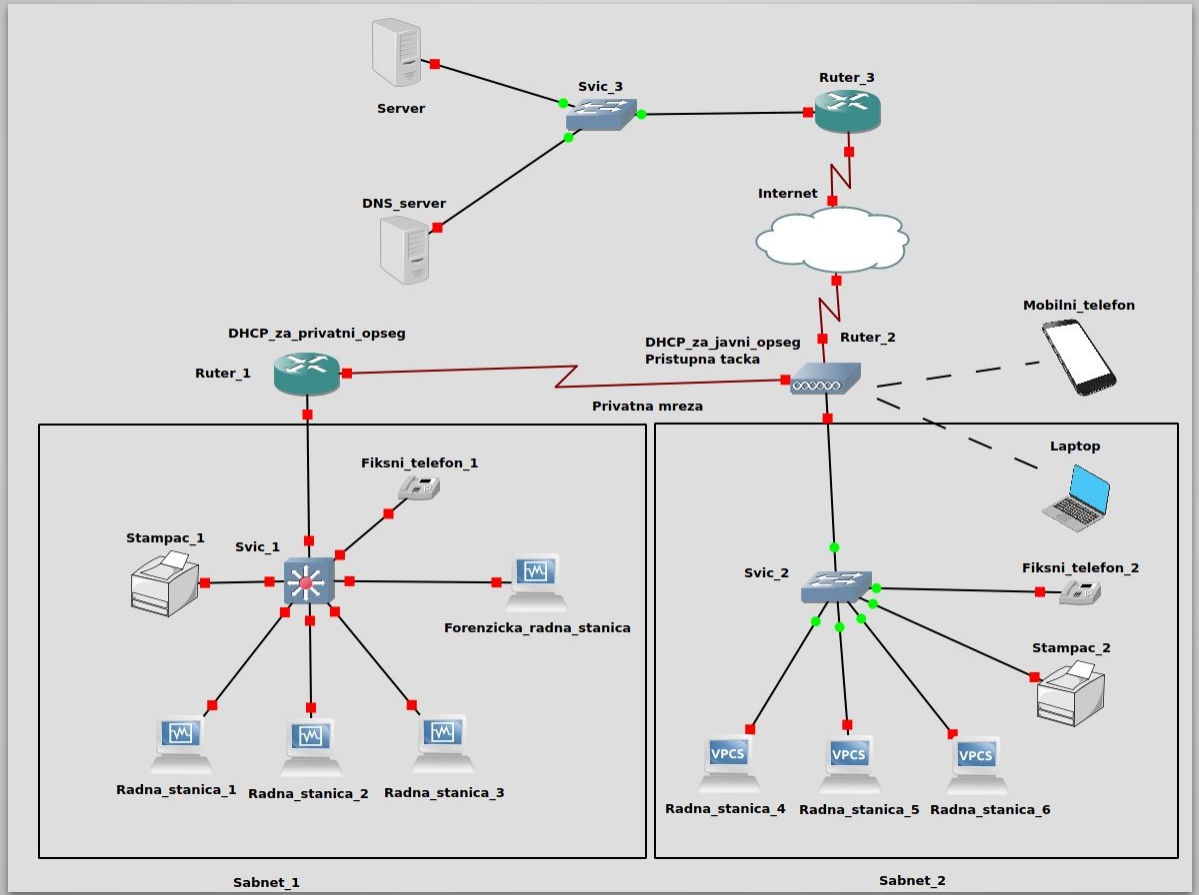
Факултет техничких наука
Лабораторија за дигиталну форензику

ФОРЕНЗИКА РАЧУНАРСКИХ МРЕЖА

Увод у дигиталну форензику

Јелена Драгишић, Светлана Антешевић

Анализа концепата рачунарске мреже



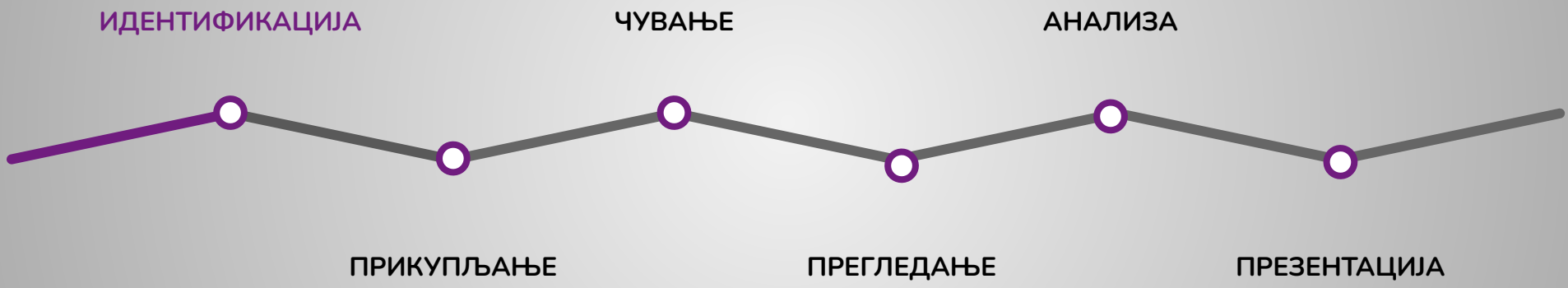
Извори доказа

- ➔ Целокупан траг пакета
- ➔ Метаподаци мрежних конекција
- ➔ Логови
- ➔ Подаци узбуне
- ➔ Статистички подаци

Мрежни уређаји

- Свич
- Хаб
- Рутер
- DHCP сервер
- DNS сервер
- Прокси сервер
- *Firewall*
- *IDS/IPS* уређаји

Процес форензичке истраге



Напомена – етапе форензичке истраге не одвијају се секвенцијално. Често су репетитивне.

Идентификација

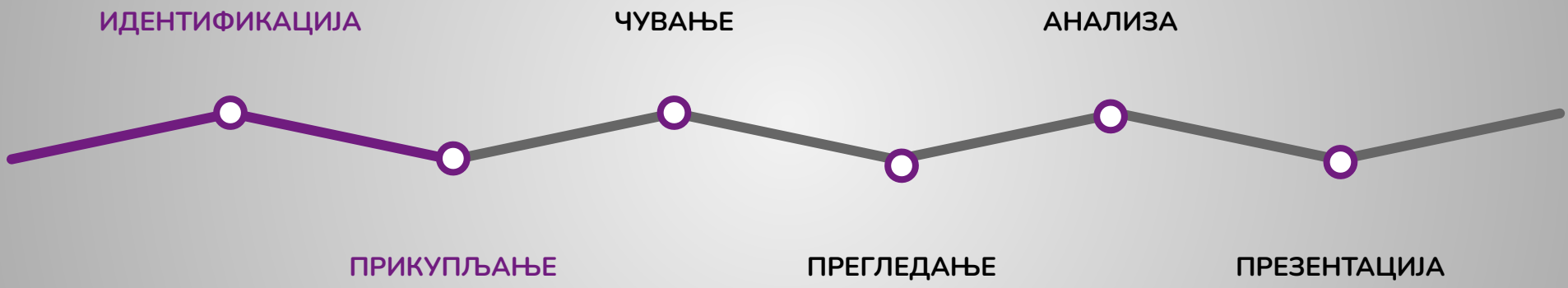
Односи се на детектовање, препознавање и одређивање дигиталних уређаја које треба истражити.

Под идентификацијом се подразумева и очитавање идентификатора дигиталних уређаја, који се истражују (произвођач, модел, серијски број).

Идентификовати све мрежне уређаје и крајње уређаје који су умрежени.

Пример: Ако постоји нека рачунарска мрежа неопходно је затражити од администратора шему мреже да бисмо имали увид у све мрежне уређаје који су коришћени, али и увид у све крајње уређаје који су умрежени.

Процес форензичке истраге



Напомена – етапе форензичке истраге не одвијају се секвенцијално. Често су репетитивне.

Прикупљање доказа

Идентификоване доказе је потребно прикупити коришћењем научно и правно ваљаних метода.

Неовлашћено прикупљање мрежног саобраћаја сматра се кривичним делом!

Потребно је припремити медије на којима се прави форензичка копија.

Прикупљање:

- ➔ Прикупљање целокупног трага пакета (жично и бежично)
- ➔ Прикупљање логова мрежних уређаја

Прикупљање целокупног трага пакета

Жично

Прислушкивачи (енг. *network tap*)

- Агрегирајући прислушкивачи
  - Сав мрежни саобраћај се копира и прослеђује на један порт.
- Регенеришући прислушкивачи
  - Мрежни саобраћај се прослеђује на више физичких портова.
- У погледу перформанси представљају најбоље решење за прикупљање мрежног саобраћаја (нема губитака пакета).

SPAN порт свича

- Конфигурација свича којом се омогућава копирање мрежног саобраћаја са одређених изворних портова свича и прослеђивање тог мрежног саобраћаја на одредишни порт свича.

- Пример конфигурације *SPAN* порта свича:

```
$ monitor session 1 source interface gi 0/2
$ monitor session 1 destination interface gi 0/1
```

- Проблем: могућност губитка пакета.


ANCHORAGE
TOKYO
DUBAI
LOS ANGELES
IMAP MODULAR
ENG D
OPER

Бежично


VECTOR
OK
INT

WiFi (IEEE 802.11)

Алат: **Wireshark**

Wireshark је GUI алат отвореног изворног кода за прикупљање, прегледање и анализу мрежног саобраћаја.

Подржава стотинак комуникационих протокола.

Омогућава снимање мрежног саобраћаја у датотеке у packet capture (PCAP) формату (и многим другим).

WiFi (IEEE 802.11)

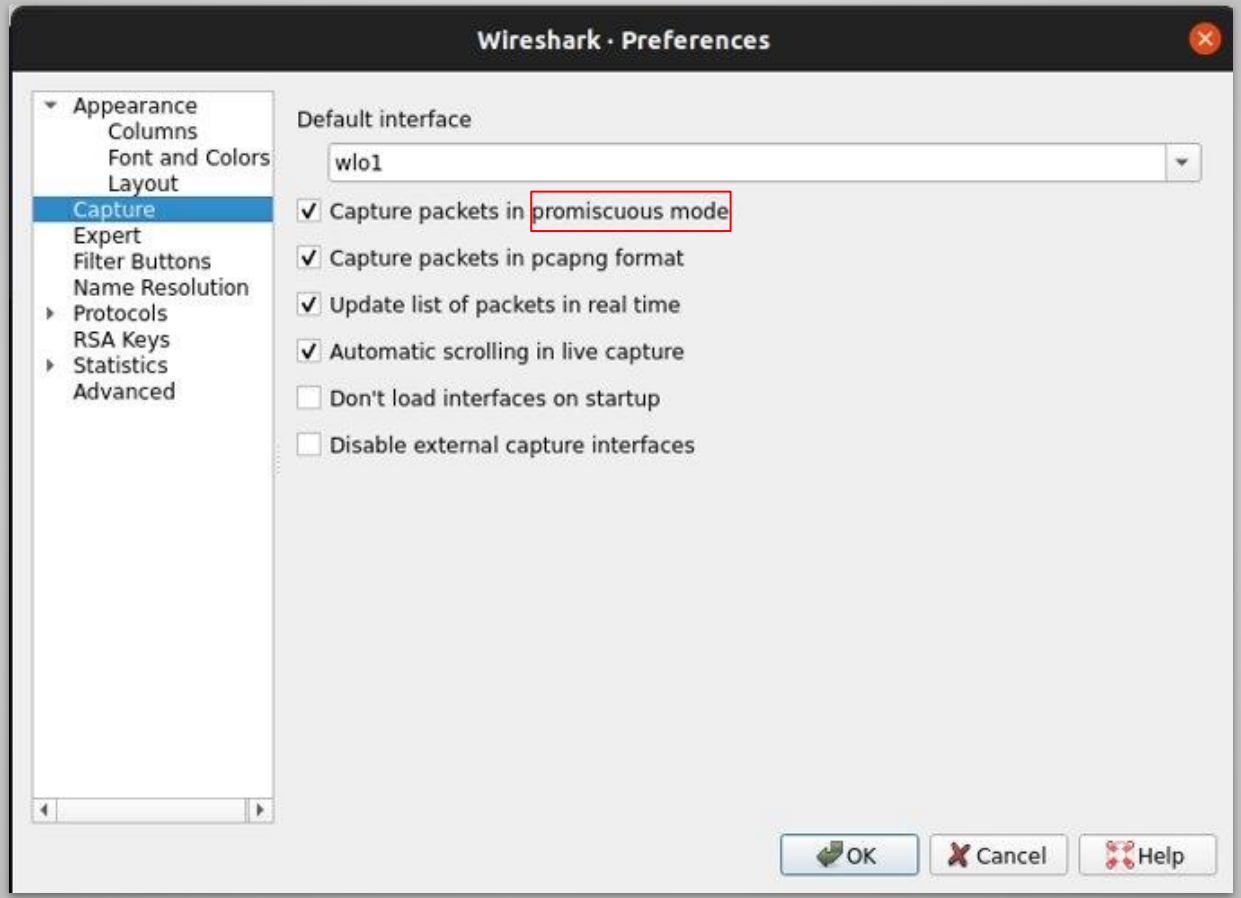
Снимање мрежног саобраћаја WiFi (IEEE 802.11) свих уређаја повезаних на исту мрежу као и рачунар на коме је покренут Wireshark, могуће је ако:

- ➔ мрежна картица подржава режим за мониторинг (promiscuous mode)
- ➔ режим за мониторинг је подешен у оквиру оперативног система

  $ sudo iwconfig wlo1 mode monitor

- ➔ режим за мониторинг је подешен у оквиру алата Wireshark

WiFi (IEEE 802.11)



Прикупљање логова мрежних уређаја

Рутер

- Основна функција рутера је рутирање.
- Команда за увид у табелу рутирања:

```
$ show ip route
```

- Резултат:

```
192.168.1.0/24 is directly connected, Serial0/0/0
192.168.2.0/24 is directly connected, Serial0/1/0
192.168.3.0/24 [120/1] via 192.168.1.1, 00:00:18, Serial0/0/0
192.168.4.0/24 [120/2] via 192.168.1.1, 00:00:18, Serial0/0/0
```

- Рутере углавном није могуће конфигурисати ради екстракције целокупних трагова пакета.
- Једноставна је конфигурација за извоз записа тока комуникације, која садржи само метаподатке мрежних конекција.

Логови DHCP сервера

- Рутер може бити конфигурисан тако да обавља функцију DHCP сервиса.
- Команда за преузимање лога DHCP сервиса:
  `$ show ip dhcp binding`
- Резултат:

IP address	Hardware address	Lease expiration	Type
172.25.1.51	0100.0103.85e9.87	Apr 10 2006 08:55 PM	Automatic
172.25.1.52	0100.50da.2a5e.a2	Apr 10 2006 09:00 PM	Automatic
172.25.1.53	0100.0103.ea1b.ed	Apr 10 2006 08:58 PM	Automatic

Логови DHCP сервера

- Linux сервер може функционисати као DHCP сервер.
- Датотека у којој се складиште логови DHCP сервиса:
  `/var/lib/dhcp/dhcpd.leases`

Логови сервиса NAT

- ➔ Рутер може бити конфигурисан тако да обавља транслирање јавна–приватна адреса.
- ➔ Ова мапирања (логови) могу да се чувају у трајној меморији рутера.
- ➔ Команда за преузимање логова NAT сервиса:

```
$ show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
tcp	192.168.1.1:514	192.168.2.3:53	192.168.2.22:256	192.168.2.22:256
tcp	192.168.1.1:513	192.168.2.2:53	192.168.2.22:256	192.168.2.22:256
tcp	192.168.1.1:512	192.168.2.4:53	192.168.2.22:256	192.168.2.22:256

Логови веб сервера

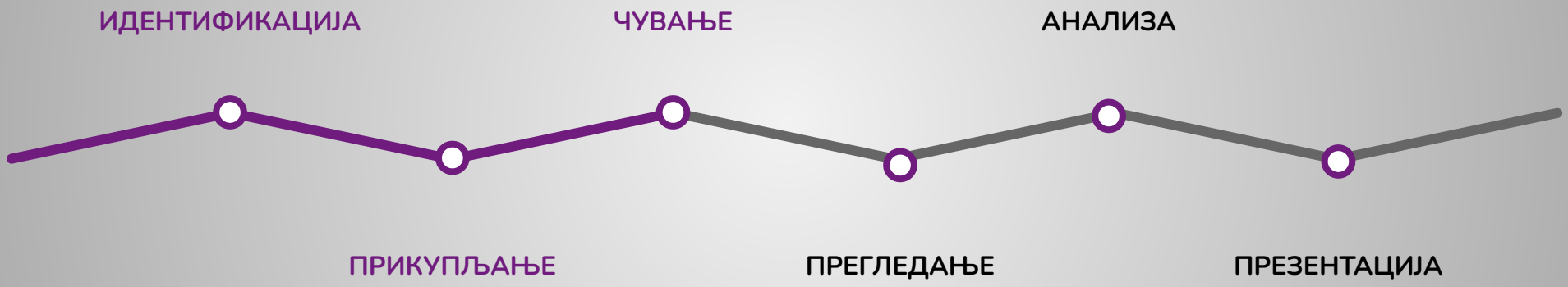
- Apache веб сервер, између осталог, поседује датотеку у којој се складиште логови приступања веб серверу: **access.log**.
- Формат записа датотеке access.log може бити:

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\""
```

- Пример једног лога:

```
127.0.0.1:8080 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif
HTTP/1.0" 200 2326 "http://www.example.com/start.html" "Mozilla/4.08 [en]
(Win98; I ;Nav)"
```

Процес форензичке истраге



Напомена – етапе форензичке истраге не одвијају се секвенцијално. Често су репетитивне.

Чување

Прикупљени докази морају се сачувати коришћењем физичких, техничких и организационих контрола.

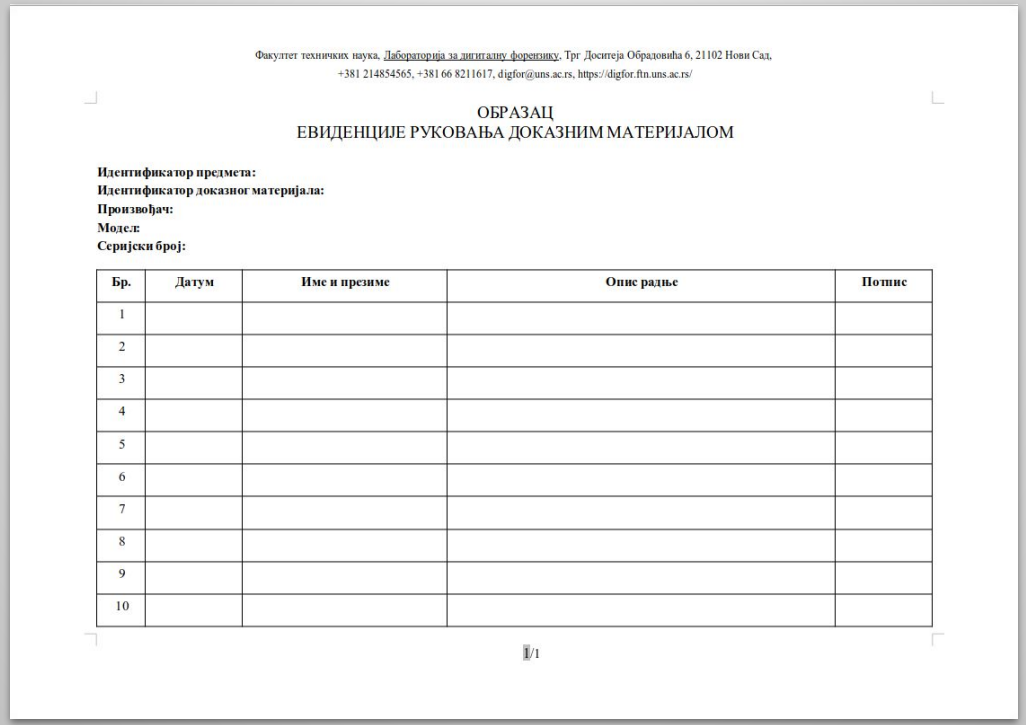
Траг мрежног саобраћаја обично се чува у датотекама формата *packet capture* (PCAP).

Рачуна се криптографска хеш вредност прикупљених доказа помоћу неких од алгоритама:

- ➔ MD5 алгоритам: **$ [sudo] md5sum [file]**
- ➔ SHA1 алгоритам: **$ [sudo] sha1sum [file]**

Чување

Ланац доказа - евиденција о томе када и ко је имао приступ доказима.



Факултет техничких наука, Лабораторија за дигиталну форензику, Трг Доситеја Обрадовића 6, 21102 Нови Сад,
+381 214854565, +381 66 8211617, digfor@uns.ac.rs, https://digfor.ftn.uns.ac.rs/

ОБРАЗАЦ
ЕВИДЕНЦИЈЕ РУКОВАЊА ДОКАЗНИМ МАТЕРИЈАЛОМ

Идентификатор предмета:
Идентификатор доказног материјала:
Произвођач:
Модел:
Серијски број:

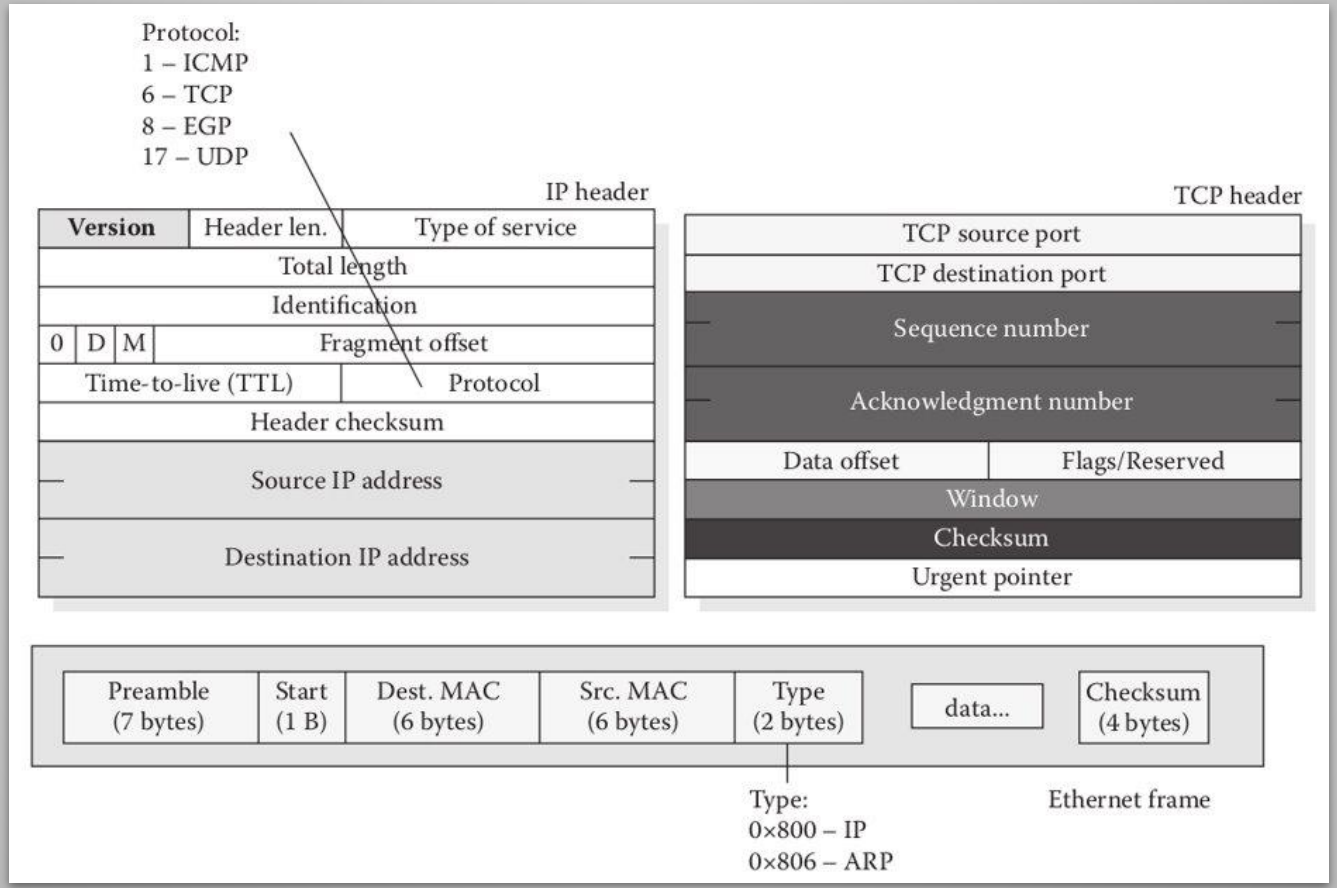
Бр.	Датум	Име и презиме	Опис радње	Потпис
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

1/1

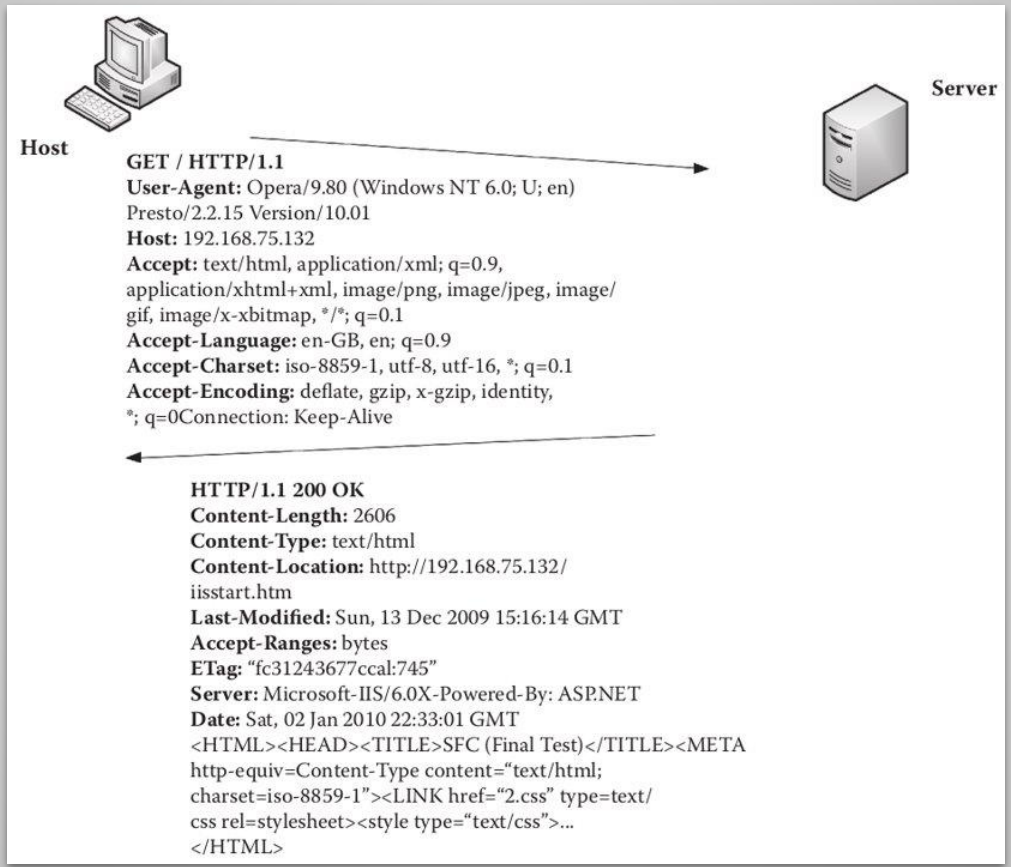
Процес форензичке истраге

Напомена – етапе форензичке истраге не одвијају се секвенцијално. Често су репетитивне.

Пакет мрежног саобраћаја



Анализа HTTP саобраћаја



Анализа заглавља електронског писма

SMTP протокол је један од најстаријих протокола апликационог нивоа; зову га још и sending and replay протокол јер обезбеђује да електронска пошта стигне до одредишне адресе.

Компоненте које учествују у реализацији овог протокола су:

- ➔ Mail User Agent - клијент који шаље електронску пошту
- ➔ Mail Submission Agent - сервер који прима електронску пошту
- ➔ Mail Transfer Agent - софтвер који прихвата и прослеђује поруке електронске поште другим релејима са којима се заједно налази на путу између пошиљаоца и примаоца
- ➔ Mail Exchanger - последњи у низу релеја (трансфера) између пошиљаоца и примаоца
- ➔ Mail Delivery Agency - клијент примаоца, који је повезан за последњим релејем, а од кога, након аутентификације прима поруку електронске поште. Ова компонента система електронске поште не имплементира SMTP протокол, већ неки од следећих: POP3, IMAP, MAPI.

Анализа заглавља електронског писма

У свакој фази испоруке електронске поште, сервер-релеј обично додаје заглавље са вредношћу за hostname и датумом и временом када је порука процесирана.

SMTP протокол је примарно у вези са TCP портом 25, али се проширује и на 587, где је неопходна аутентификација.

SMTP није иницијално замишљен да подржава размену фајлова, слика и других типова садржаја, сем текстуалног. Зато је усвојен MIME стандард (Multipart Internet Mail Extension), који прописује бележење граница сегмената (boundaries) у заглављу пакета. Свака граница указује на сегмент пакета са посебним типом садржаја, што је нарочито значајно при екстракцији садржаја прилога у виду датотека.

Анализа заглавља електронског писма

Return-Path: <adresa2@domen2.com>;
Delivered-To: adresa1@domen1.rs;
Received: from budo120.adriahost.com; by budo120.adriahost.com with LMTP; id oIqnAKPzXmHyYDAA4dcWOg; (envelope-from <adresa2@domen2.com>); for <adresa1@domen1.rs>; Thu, 07 Oct 2021 15:18:27 +0200;
Return-path: <adresa2@domen2.com>;
Envelope-to: adresa1@domen1.rs;
Delivery-date: Thu, 07 Oct 2021 15:18:27 +0200;
Received: from mail-oi1-f171.google.com ([209.85.167.171]:42676); by budo120.adriahost.com with esmtps (TLS1.2) tls TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256; (Exim 4.94.2);
id 1mYTI1-00DN4H-Pd; for adresa1@domen1.rs; Thu, 07 Oct 2021 15:18:26 +0200;
Received: by mail-oi1-f171.google.com with SMTP id g125so2218127oif.9; for <adresa1@domen1.rs>; Thu, 07 Oct 2021 06:18:05 -0700 (PDT);
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;; d=domen2.com; s=google;; h=mime-version:references:in- reply-to:from:date:message-id:subject:to; :cc;; bh=TIfN1RNyojbDDsBuqygtGYpvnDnpv6kIsTEOUcYgENA=;;
b=1kwDls5WPGnawEayzzeKhEH00isxfSx6h5uBLFB9trzxShRM5pdKveg+n2MO0n+xwP;
zC7vCkr/odb/3h1R9ACriv67jTSr549yIkoooD46mt4iFAQ4S6V35iKbNHu5Fj8W8mDR;
dwRraN5EzLuw1HKobIygLbygkGw2jzH67DYwE=; X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;; d=1e100.net; s=20210112;; h=x-gm-message-state:mime-version:references:in-reply-to:from:date; :message-id:subject:to:cc;;
bh=TIfN1RNyojbDDsBuqygtGYpvnDnpv6kIsTEOUcYgENA=;;
b=Kq1RnltWBrMYuiEPEpUhBpiitXwqBwkPZTasIaWk4SGoQ1HreZexFiVnR2XTnTC995;
u0dPwupuzSjTdwRbrSwriqcamWQFIxgKniq9HxMVVDrtyq6Dp9n2vRKdzGIY6+o3FNwZ;
y39HY5MhsOhTrAId1eWYsEsPv5Vg8dgkJs58zdS53cX8Qi+KKDq0QcuXZ3XTQWHTdtI/;
Po4b33emha0SJK14i38IX5CC9h0HmTEvuajiSYuwbtdDbICTizNeMcr8huvjoxLV38w5;

Анализа заглавља електронског писма

```
    zf4I+TmpS15MmTT+PF1WaYCodaFqviJ8jnhfottBZDTWQkh5OznJL9gkvPO+LceNS8VT;        giVg==; X-Gm-Message-State:
    AOAM532YfkHfYyEtfe5TdJFZK5KXWSUvuOOYQbXXSPGWmuLyj+dqbgx1;
    drOOkC/d7l8F/Axpg6bMSNwz8M3H6y6qD8s/a/L7HatZOWOavKyN;
X-Google-Smtp-Source:
    ABdhPJxNmZtL8+LAFKBhk6YIaubhQlnXvO5cNDMuoOET5zyClagVOw5MjlYKt2zP2IY5ZvzjxNpJUdTM04+PDPK270g=; X-
Received: by 2002:aca:f283:: with SMTP id q125mr11309413oih.172.1633612663295;;  Thu, 07 Oct 2021 06:17:43 -0700 (PDT);
MIME-Version: 1.0;
References: <!&!
    AAAAAAAAAAAuAAAAAAAAAANQ7BEzjV5BPpT2DDR1ckVkBAMO2jhD3dRHOtM0AqgC7tuYAAAAAAA4AABAAAAAa9Q2oWQiPQ
    pO4qq4kipQfAQAAAAA=
In-Reply-To: <!&!
    AAAAAAAAAAAuAAAAAAAAAANQ7BEzjV5BPpT2DDR1ckVkBAMO2jhD3dRHOtM0AqgC7tuYAAAAAAA4AABAAAAAa9Q2oWQiPQ
    pO4qq4kipQfAQAAAAA=
From: Ime2 Prezime2 <adresa2@domen2.com>;
Date: Thu, 7 Oct 2021 15:17:16 +0200;
Message-ID: <CAFUq=0=D6f0uqVWeKN5jcmu3b8ioh3quHZ+BoTCZgPQ8f9s9uA@mail.gmail.com>;
Subject: Re: FW:
To: Ime1 Prezime1 <adresa1@domen1.rs>;
Cc: "Ime3 Prezime3" <adresa3@domen2.com>;
Content-Type: multipart/mixed; boundary="0000000000007f423c05cdc31621"; ;
```

Анализа заглавља електронског писма

Алат: **NetworkMiner**

Network Miner је GUI софтверски алат отвореног изворног кода за прегледање и анализу ”живог” мрежног саобраћаја или сачуваних трагова мрежног саобраћаја.

Подржава многе комуникационе протоколе, укључујући: TCP, UDP, HTTP, SIP, POP3, IMAP, SMTP итд.

Аутоматизује парсирање мрежног саобраћаја и приказује податке на интуитиван начин (нпр. датотеке, фотографије, поруке, креденцијали, сесије итд.)

Користи се за: анализу електронске поште, реконструкцију корисничке сесије, ...

Анализа заглавља електронског писма

Алат: **NetworkMiner**

Покретање:

$ cd /opt/NetworkMiner_2-7-2

$ mono NetworkMiner.exe

Информације о имену домена

Алат: **whois**

WHOIS је сервис за постављање упита над базама података које складиште податке о интернет ресурсима (као што је и име домена).

WHOIS је широко коришћена листа интернетских записа која идентификује ко је власник домена и како да ступи у контакт са њим.

Интернет корпорација за додељена имена и бројеве (ICANN) регулише регистрацију назива домена и власништво.

$ whois <naziv_domena>

Информације о имену домена

```
Domain name: ac.rs
Domain status: Active https://www.rnids.rs/en/domain-name-status-codes#Active
Domain status: Registry lock
https://www.rnids.rs/en/domain-name-status-codes#Registry_lock
Domain status: serverUpdateProhibited
https://www.rnids.rs/en/domain-name-status-codes#ServerUpdateProhibited
Registration date: 10.03.2008 12:00:00
Modification date: 01.04.2019 12:07:07
Expiration date: 10.03.2108 12:00:00
Confirmed: 10.03.2008 12:00:00
Registrar: RNIDS

Registrant: RNIDS
Address: Žorža Klemansoa 18a, Beograd, Serbia
Postal Code: 11000
ID Number: 17680544
Tax ID: 104852190
```

Информације о имену домена

Administrative contact: RCUB - Računski centar Univerziteta u Beogradu
Address: Kumanovska bb, Beograd, Serbia
Postal Code:
ID Number:
Tax ID:
Technical contact: RCUB - Računski centar Univerziteta u Beogradu
Address: Kumanovska bb, Beograd, Serbia
Postal Code:
ID Number:
Tax ID:
DNS: odisej.telekom.rs - 195.178.32.2
DNS: ns.rcub.bg.ac.rs - 147.91.1.5
DNS: gaea.rcub.bg.ac.rs - 147.91.1.7
DNS: ns1.uns.ac.rs - 147.91.173.4
DNS: ban.junis.ni.ac.rs - 160.99.1.1
DNS: ns.unic.kg.ac.rs - 147.91.209.2
DNS: ns.etf.bg.ac.rs - 147.91.8.6
DNS: ns2.iif.hu - 193.225.12.59
DNSSEC signed: no
Whois Timestamp: 09.02.2022 06:01:34

Процес форензичке истраге

Напомена – етапе форензичке истраге не одвијају се секвенцијално. Често су репетитивне.

Презентација

Резултати анализе доказа се презентују у писменом облику.

Односи се на процес којим форензичар дели резултате фазе анализе у облику извештаја заинтересованим странама.

Форензичар обично сачињава налаз и мишљење и усмено га брани одговарајући на питања на главном судском претресу.

Коришћени алати

- Wireshark https://www.wireshark.org/
- NetworkMiner https://www.netresec.com/
- whois
- *Digital Forensics with Kali Linux*
- *Digital forensics : an academic introduction*