OFFICE OF ANTITERRORISM ASSISTANCE

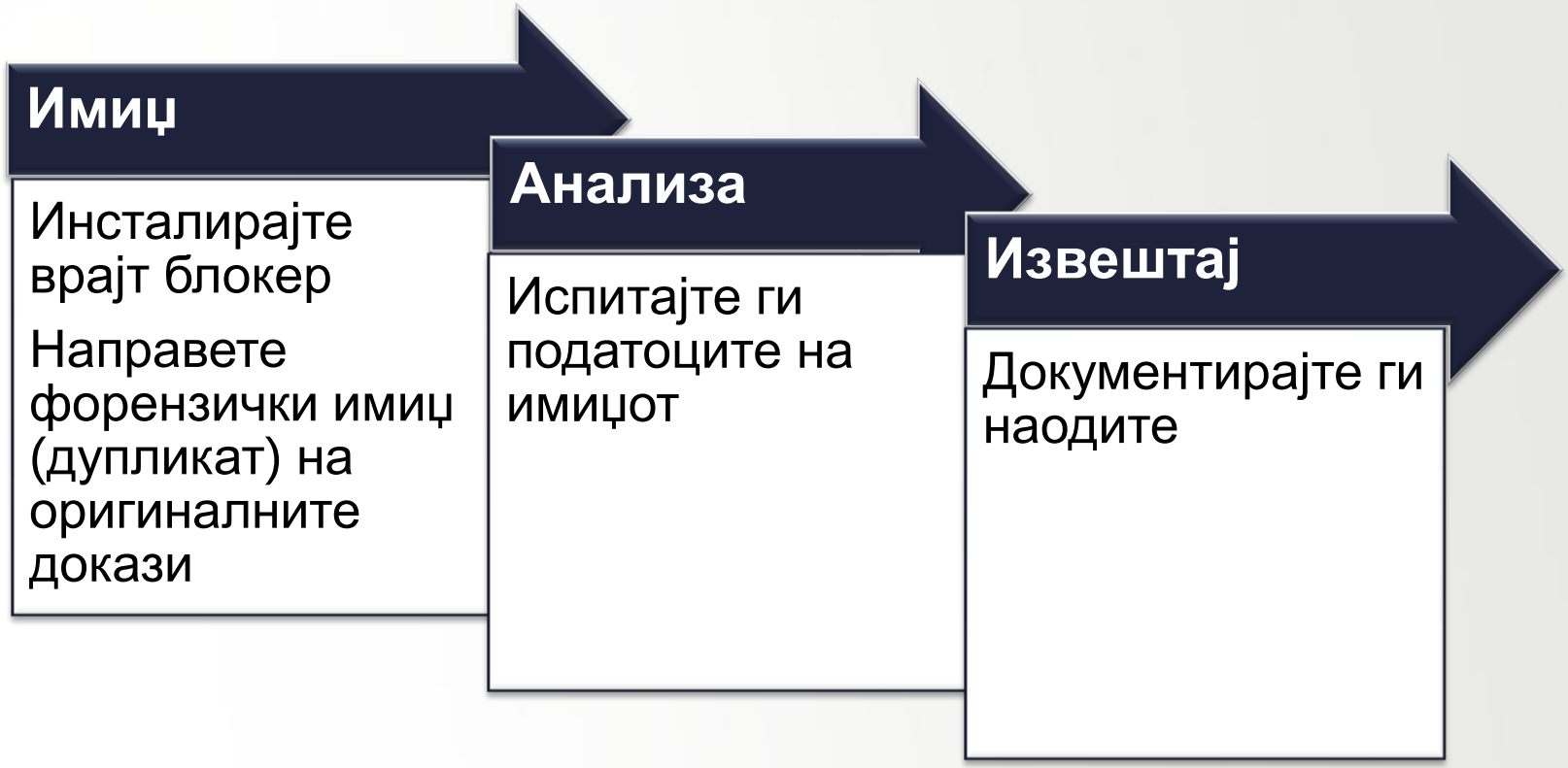
Модул 6

Анализа на дигитални докази

Цел на модулот

- До крајот на овој модул ќе научите како да ги процените процедурите за анализа кои ги користеле вештаците

Преглед на процесот на анализа



Правење имиџ: Врајт блокери (Write Blockers)

- Ги штитат оригиналните докази
- Им овозможуваат на вештаците да ги читаат податоците без да ги менуваат

Source: US Fish & Wildlife Service

Source: US Fish & Wildlife Service

Правење имиџ: Дуплицирање на податоци

- Се користи специјализиран софтвер за да се направи форензички имиџ —идентичен дупликат
- Се складира имиџот на форензички пребришан уред
- Се верификува дали имиџот соодветствува на оригиналот
- Се анализира имиџот, а оригиналот се складира

Правење имиџ: Хаш (Hash) вредности

- Внесување на податоци во хаш функцијата (математичка формула) за да се назначи единствена хаш вредност
- Најчести примери се MD5 и SHA1

Примери за хаш вредности

Правење имиџ: Проверка на хаш

Оригинални докази

Извор: Getty Images

Хаш функција → **Хаш вредност**

Идентичната хаш вредност докажува дека податоците се идентични

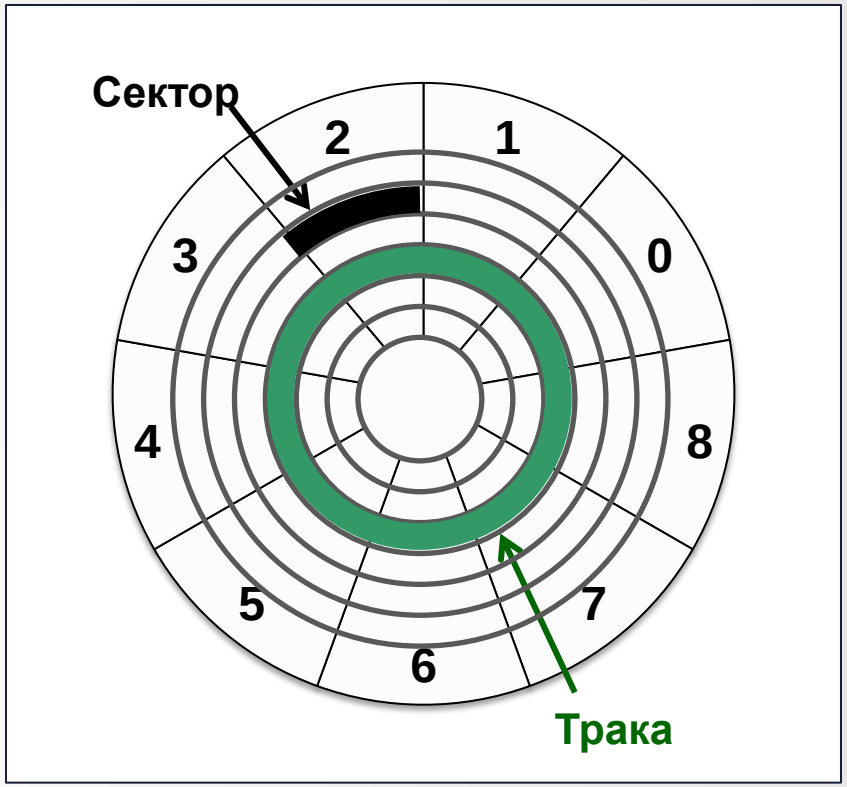
Форензички имиџ

Извор: Getty Images

Хаш функција → **Хаш вредност**

Анализа: Лоцирање на податоците

- Податоците може да се каде било на хард дискот
- Постои табела која евидентира каде се складирани податоците
- Избришаните податоци остануваат на дискот, но се означени како избришани во табелата



Анализа: Специјализирани алатки

- Со форензички алатки може да се лоцираат и вратат избришаните податоци
- Овие алатки исто вршат и низа други задачи за форензичка анализа

Вредноста на форензичките алатки

- **Дигиталните медиуми содржат огромни количества податоци**
- **Форензичките алатки ја насочуваат потрагата по докази**

CD = 650 MB (440,000 страници со податоци)

Паметен (смарт) телефон = 64 GB (43,000,000 страници со податоци)

Хард диск драјв = 1 TB (675,000,000 страници со податоци)

Техники: Хаш анализа

- **Идентичните фајлови имаат иста хаш вредност**
- **Вештаците ги чуваат датабазите на познатите фајлови:**
  - **Брзо да ги лоцираат фајловите со доказна вредност**
  - **за да ги игнорираат фајловите што немаат доказна вредност за да заштедат време**

Техники: Пребарување по индекс

- Форензичките алатки ги индексираат сите зборови и знаци (карактери) во медиумот
- Вештаците може веднаш да пребаруваат клучни зборови

Source: Getty Images

Техники: Враќање на избришани фајлови

- Податоците што се означени како избришани и понатаму остануваат на хард дискот освен ако не се препише врз нив
- Форензичките алатки ги лоцираат и враќаат избришаните фајлови

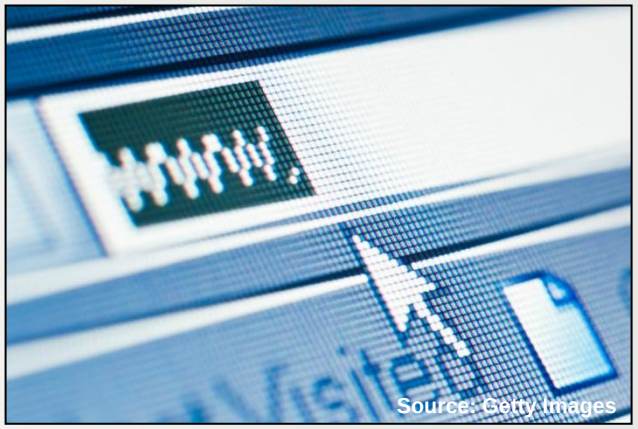
Source: Getty Images

Техники: Потписи и екстензии на фајлови

- Типот на фајл се препознава по:
  - Потписнички код на почетокот на фајлот
  - Екстензијата на крајот на фајлот
- Форензичките алатки идентификуваат несовпаѓања — потпис што не соодветствува на екстензијата

Техники: Интернет историја и кеш (Cache)

- **Компјутерите можат:**
  - **Да ги евидентираат посетените страници на интернет**
  - **Да чуваат привремени копии на посетени слики и страници**



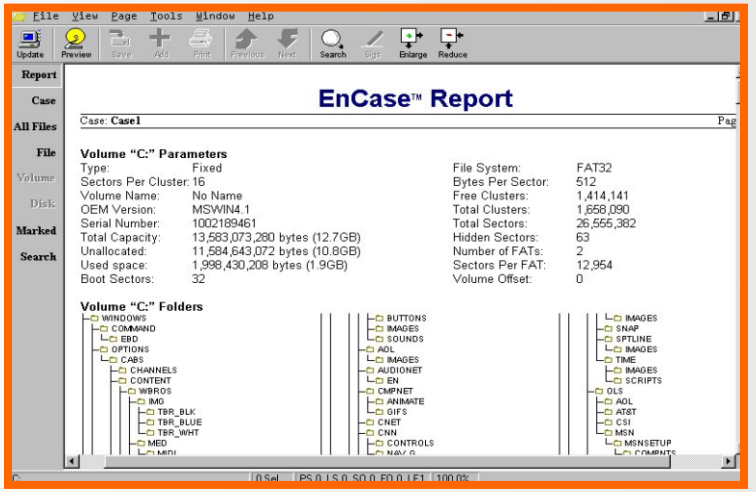
- **Со форензичките алатки може да се вратат овие информации за да се помогне да се реконструира активноста на интернет**

Техники: Windows Регистер

- Windows користи датабаза која се нарекува регистер за да води евиденција за информациите за конфигурацијата
- Со форензичките алатки може да се вратат докази како:
  - Системска временска зона
  - Активност на логирање
  - Инсталирани апликации
  - Фајлови до кои неодамна е пристапено
  - Надворешни медиуми приклучени на компјутерот

Извештајот од компјутерското вештачење

- Опис на дигиталните медиуми
- Датумите на подигање и вештачење
- Хаш верификација
- Системски информации
- Windows регистер (фолдери)
- Важни прикачени податоци, со локација



Студија на случај: Толкување на извештајот од анализата

Погледни: Прирачник (Активност #3)

- **Инструкции: Работа во тимови:**
  - **Прегледајте ги информациите од претходниот случај и земете ги предвид новите детали дадени во прирачникот**
  - **Одговорете ги прашањата за дискусија**
  - **Подгответе се да ги споделите одговорите за 45 минути**

Студија на случај: финална дискусија

- Вредност на непостојаните податоци?
- Методи на пребарување? Вредност на избришаните податоци?
- Форензички софтвер?
- Вкупен капацитет на податоците? Значење?
- Техники за да се спречи менување на податоците?
- Прашања до вештакот?

Резиме на модулот

Погледнете:
Прилог 6.1

- **Собирање дигитални докази**
- **Анализа на дигитални докази**
- **Толкување на извештаите и наодите**