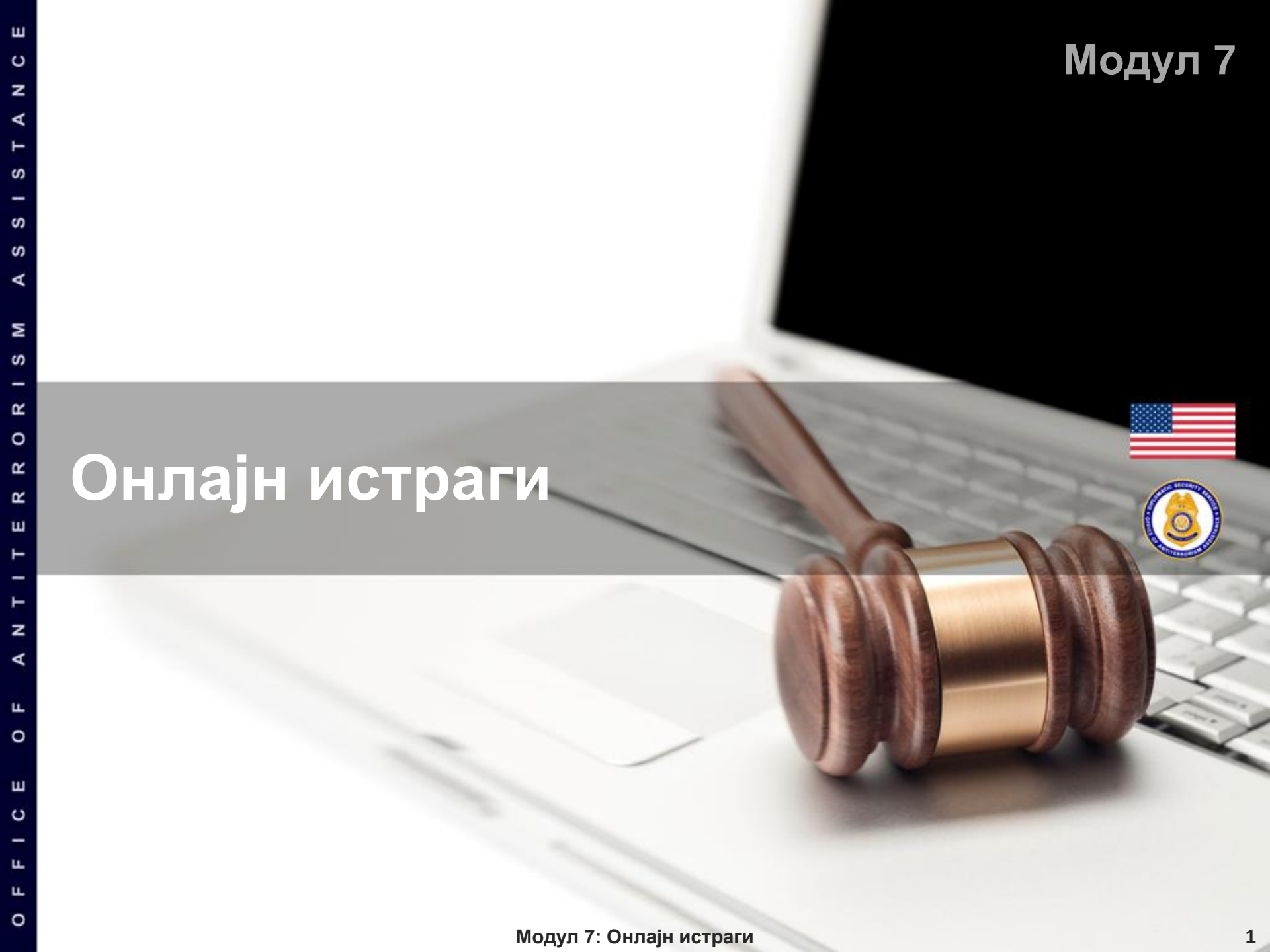
OFFICE OF ANTITERRORISM ASSISTANCE

Модул 7

Онлајн истраги



Цел на модулот

- До крајот на овој модул ќе знаете како да ги анализирате процедурите за онлајн истраги и наодите кои произлегуваат од нив за да утврдите дали добиените информации може да се користат како докази

Вредноста на истрагите преку интернет

- **Современиот живот се одвива онлајн, со што се остава дигитална трага**
- **Компјутерските истражители ја идентификуваат криминалната активност анализирајќи:**
  - **Информации на интернет од отворен карактер**
  - **Онлајн докази од интернет сервис провајдери**

Процесот на вршење онлајн истраги

Собирање

Проучете ја онлајн активноста

Соберете ги и менаџирајте ги онлајн доказите

Координирање

Работете со истражители и вештаци

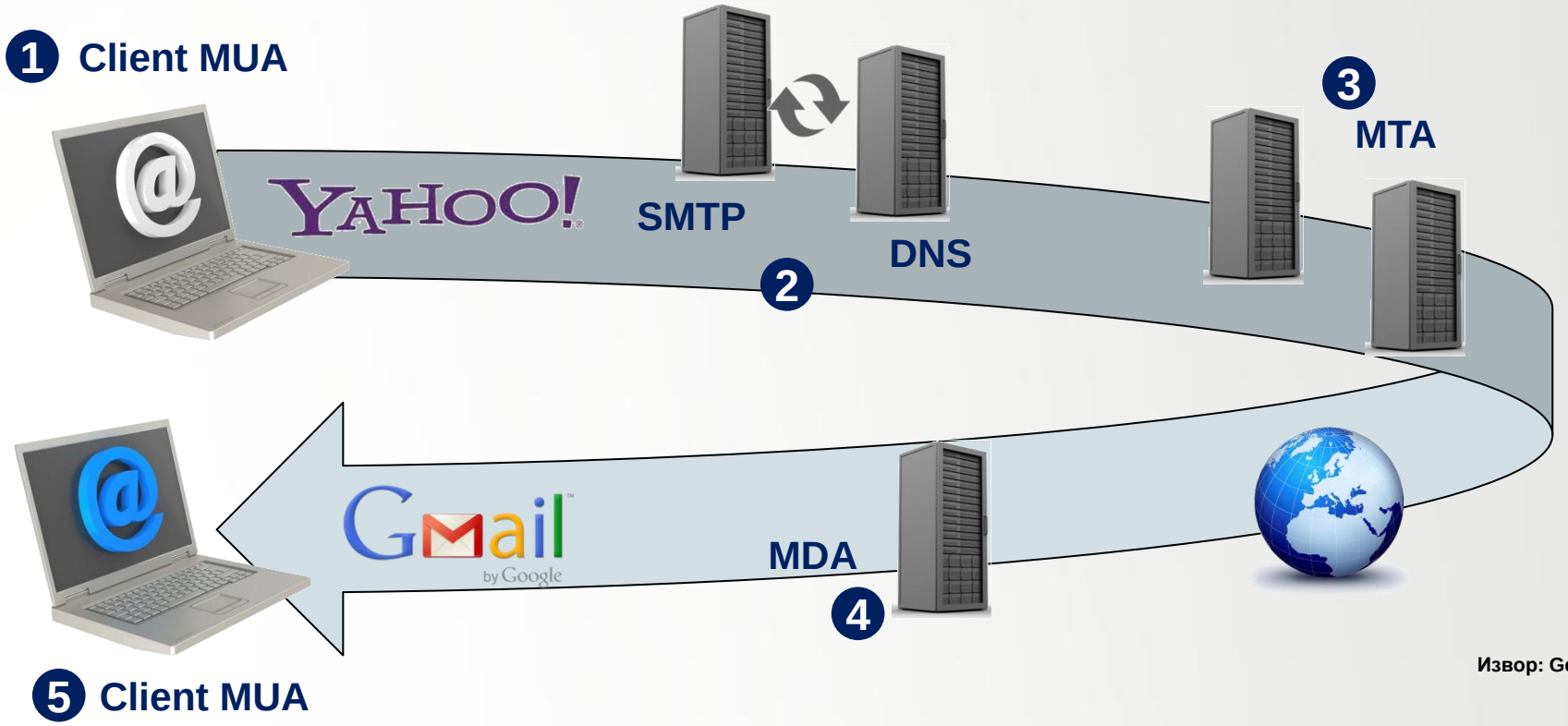
Побарајте информации за претплатникот

Известување

Анализирајте ги доказите

Документирајте ги наодите

Преглед: Email Routing



Извор: Getty Images

Key:

Mail User Agent (MUA)
Simple Mail Transfer Protocol (SMTP)
Domain Name Server (DNS)
Mail Transfer Agent (MTA)
Mail Delivery Agent (MDA)

Преглед: Хедери на е-пошта

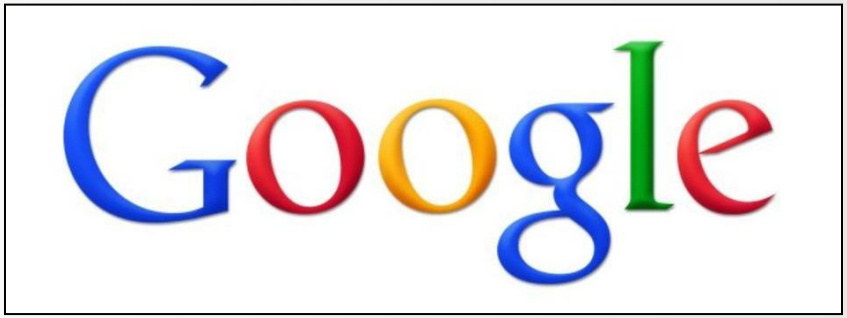
Delivered-To: recipientgmail.com
Received: by 10.204.24.211 with SMTP id w19csp20849bkb;
Sat, 27 Jul 2013 07:31:37 -0700 (PDT)
Return-Path: <k*llyou54234@yahoo.com>
Received: from nm1-vm0.bullet.mail.ne1.yahoo.com (nm1-vm0.bullet.mail.ne1.yahoo.com. [98.138.91.74])
by mx.google.com with ESMTPS id u9si23440266yhg.16.2013.07.27.07.31.36
for <recipient@gmail.com> (Sat, 27 Jul 2013 07:31:37 -0700 (PDT)
Received: from [98.138.90.52] by nm1.bullet.mail.ne1.yahoo.com with NNFMP; 27 Jul 2013 14:31:31 -0000
Received: from [98.138.101.167] by tm5.bullet.mail.ne1.yahoo.com with NNFMP; 27 Jul 2013 14:31:31 -0000
Received: from [127.0.0.1] by omp1078.mail.ne1.yahoo.com with NNFMP; 27 Jul 2013 14:31:31 -0000
Received: from [94.205.104.234] by web120404.mail.ne1.yahoo.com via HTTP; Sat, 27 Jul 2013 07:31:30 PDT
Date: Sat, 27 Jul 2013 07:31:30 -0700 (PDT)
From: anonymous person <k*llyou54234@yahoo.com>
Subject: I will kill you
To: “recipient@gmail.com" <recipient@gmail.com>

Преглед: Веб сајтови

- Веб сајтовите често содржат релевантни докази
- Компјутерските истражители ја пребаруваат:
  - Датабазата WhoIs за регистрираниот сопственик
  - IP адресата на хостот за географската локација

Преглед: Пребарувачи

- **Истражителите користат пребарувачи за разузнавачки сознанија од отворен карактер, како:**
  - **Тековна криминална активност**
  - **Детали за конкретни осомничени што се објавени онлајн**



Преглед: Социјални медиуми

- Сајтовите на социјалните медиуми содржат огромни количества информации
- Истражителите бараат или следат:
  - Криминални организации
  - Терористички групи
  - Поединечни осомничени

Source: Getty Images

Преглед: Докази на интернет

- Многу компјутери кои нудат онлајн услуги вршат следење на активноста
- Истражителите може да најдат:
  - Записи на веб страници (логови на веб страници)
  - Евиденција за претплатници на Интернет сервис провајдерот
  - Записи од пристап до е-пошта
  - Евиденција за доделување на IP адреси

Добивање информации за претплатникот

- Во барањето бидете што е можно попрецизни
- Одговорите може да содржат:
  - Доделување на IP адреси
  - Е-пошта
  - Евиденција за трансакции

Пример: Одговор на Интернет Сервис Провајдерот (ISP)

- **Провајдерите сами решаваат кои податоци ќе ги евидентираат и чуваат**
- **Податоците што ги дал корисникот може да не се проверени**

YAHOO!

Yahoo! Account Management Tool

Login Name:	wallabee74
Properties Used:	Mail
Yahoo Mail Name:	wallabee74@yahoo.com
(Alternate) Email Address:	
Registration IP Address:	66.191.249.13
Account Created (reg):	Fri Nov 10 15:59:52 GMT
Other Identities:	wallabee74 (Yahoo! Mail)
Full Name:	Mr. John Doe
Address 1:	
Address 2:	
City:	Pigeon Forge
State, Territory or province:	TN
Country;	United States
Zip/Postal Code:	37863
Phone:	
Time Zone:	Ct
Account Status:	Active

Search in all for: wallabee74

Yahoo! Login Tracker:

Search Results

Login	IP Address	Day	Date	Time	Time Zone
wallabee74	75.46.75.81	Sun	2007-07-15	03:01:54	GMT (GMT+0000)
wallabee74	75.46.75.81	Tue	2007-07-17	19:28:50	GMT (GMT+0000)
wallabee74	75.46.75.81	Tue	2007-07-17	20:06:40	GMT (GMT+0000)
wallabee74	75.46.75.81	Wed	2007-07-18	03:37:50	GMT (GMT+0000)
wallabee74	75.46.75.81	Thu	2007-07-19	00:03:49	GMT (GMT+0000)

Активност: Евиденција на ISP за претплатникот

Погледнете: Addendum 7.1

- **Инструкции: Работа во тимови:**
  - **Прегледајте ги информациите за претплатникот добиени од ISP**
  - **Одговорете ги прашањата за дискусија**
  - **Подгответе се да ги споделите одговорите за 10 минути**

Активност: Разработка

- **Во примерот Great Works Internet, кои се важните:**
  - **Временски ознаци?**
  - **IP адреси?**

gwi
Great Works Internet

Name:	AlbertXXXXXXXXXX [REDACTED]
Username:	Daddyankee
Email:	daddyankee@gwi.net
Address:	210XXXXXXX Street, Apartment 3 [REDACTED]
	Rumford, Maine 04276
Phone:	207-XXX-XXXX [REDACTED]
Birthday:	XX/XX/1979 [REDACTED]
Payment Method:	
	Credit Card: Visa
	Number: XXXX-XXXX-XXXX-XXXX [REDACTED]
	Exp. 08/2010
Customer Since:	6/14/2004
Details from Logs:	
	66.55.208.134 is the IP of our Rumford DSL equipment
	00:0f:db:be:a7:b6 is the MAC address of the customers computer or router
	bir-1-33 is the card and modem number this customer is connected through

Logs:

Jan 29 12:06:58	DHCPUSER: 00:0f:db:be:a7:b6 Chassis: 66.55.208.134 IP:205.94.63 Circuit ID:bir-1-33
Jan 29 12:06:58	DHCPREQUEST for 205.209.94.63 from 00:0f:db:be:a7:b6 via 66.55.208.134
Jan 29 12:06:58	DHCPACK on 205.209.94.63 to 00:0f:db:be:a7:b6 via 66.55.208.134
Jan 29 13:06:58	DHCPUSER: 00:0f:db:be:a7:b6 Chassis: 66.55.208.134 IP:205.94.63 Circuit ID:bir-1-33
Jan 29 13:06:58	DHCPREQUEST for 205.209.94.63 from 00:0f:db:be:a7:b6 via 66.55.208.134
Jan 29 13:06:58	DHCPACK on 205.209.94.63 to 00:0f:db:be:a7:b6 via 66.55.208.134
Jan 29 14:06:58	DHCPUSER: 00:0f:db:be:a7:b6 Chassis: 66.55.208.134 IP:205.94.63 Circuit ID:bir-1-33
Jan 29 14:06:58	DHCPREQUEST for 205.209.94.63 from 00:0f:db:be:a7:b6 via 66.55.208.134
Jan 29 14:06:58	DHCPACK on 205.209.94.63 to 00:0f:db:be:a7:b6 via 66.55.208.134

Преглед: Предизвици

- **Онлајн истрагите може да бидат попречени од:**
  - **Анонимни системи на е-пошта (препраќачи - remailers)**
  - **Интернет кафулиња**
  - **Wi-Fi со слободен пристап**
  - **Друг анонимен пристап до интернет**
- **За да се поврзе осомниченият со кривичното дело може да се потребни и традиционалните полициски техники**

Алатки и техники

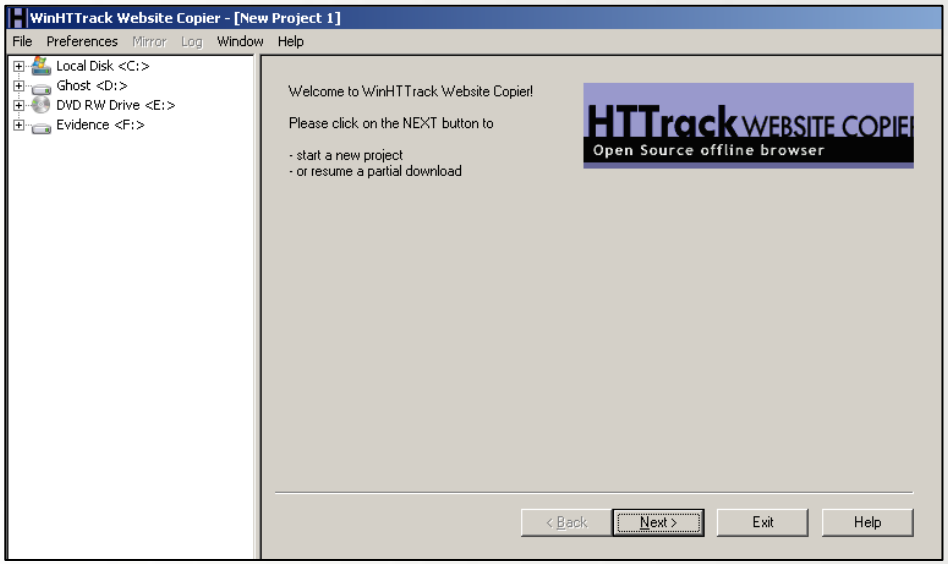
- **Онлајн истрагите:**
  - **Може да се долги**
  - **Може да опфатат собирање докази од многу извори**
- **Истражителите треба да спроведат контроли за прецизност и отчетност**

Техники: Снимање на екран

- Алатките ја снимаат онлајн активноста како што се покажува на екранот
- Овие алатки се слични на камера што ја снима активноста во физичкиот свет

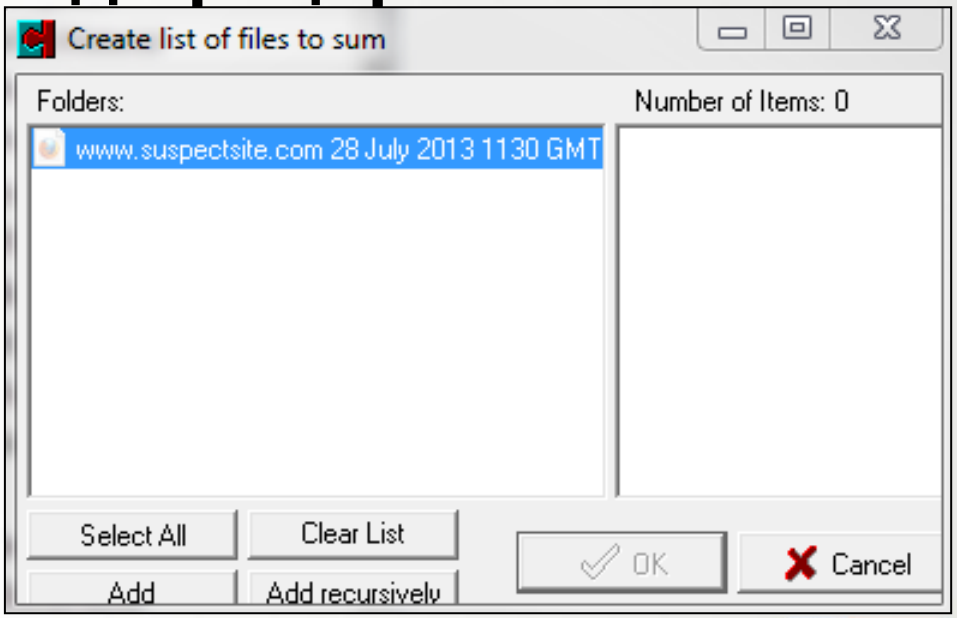
Техники: Спуштени фајлови и офлајн веб страници

- **Алатките како HTTrack:**
  - **Директно ги спуштаат веб страниците и фајловите што се постирани онлајн**
  - **Создаваат дигитален приказ на содржината за одреден ден и време**



Техники: Хаш функција

- По спуштањето на одредени онлајн фајлови и зачувувањето на слики од екранот, истражителите ги хашираат фајловите.
- Тоа се користи за да се покаже дека фајловите не се модифицирани по собирањето.



Техники: Фајлови за пристап (лог фајлови)

- Многу уреди автоматски создаваат записи за пристап (логови)
- Истражителите може:
  - Да ги ископираат фајловите од серверот и да го пресметаат нивниот хаш
  - Да направат логички имиџ на фајловите

Ракување со докази

- **Истражителите треба да ги контролираат доказите користејќи:**
  - **Форензички пребришани (чисти) медиуми**
  - **Медиуми наменети само за еден предмет**
  - **Доследна структура на фајловите**

Source: Getty Images

Анализа и известување

- **Обучените истражители:**
  - **Ги анализираат доказите**
  - **Користат специјализиран софтвер, според потребите (како анализа на записи/ логови)**
  - **Известуваат за резултатите**


Source: Getty Images

Студија на случај: Толкување на ISP одговори

Погледнете: Прирачник (Активност #4)

- **Инструкции: Работете во тим:**
  - **Разгледајте ги информациите од претходната студија на случај и земете ги предвид новите детали дадени во прирачникот**
  - **Одговорете на прашањата за дискусија**
  - **Подгответе се да ги споделите одговорите за 30 минути**

Студија на случај: Финална дискусија

- Како вие би го утврдиле кредибилитетот на информациите?
- Кои докази би ги извеле? Како е тоа поврзано со наодите на вештакот?
- Какви прашања би му поставиле на компјутерскиот истражител?

Резиме на модулот

Погледнете:
Прилог 7.2

- **Процесот на онлајн истраги**
- **Алатки и техники**
- **Одговори на Интернет сервис провајдери**