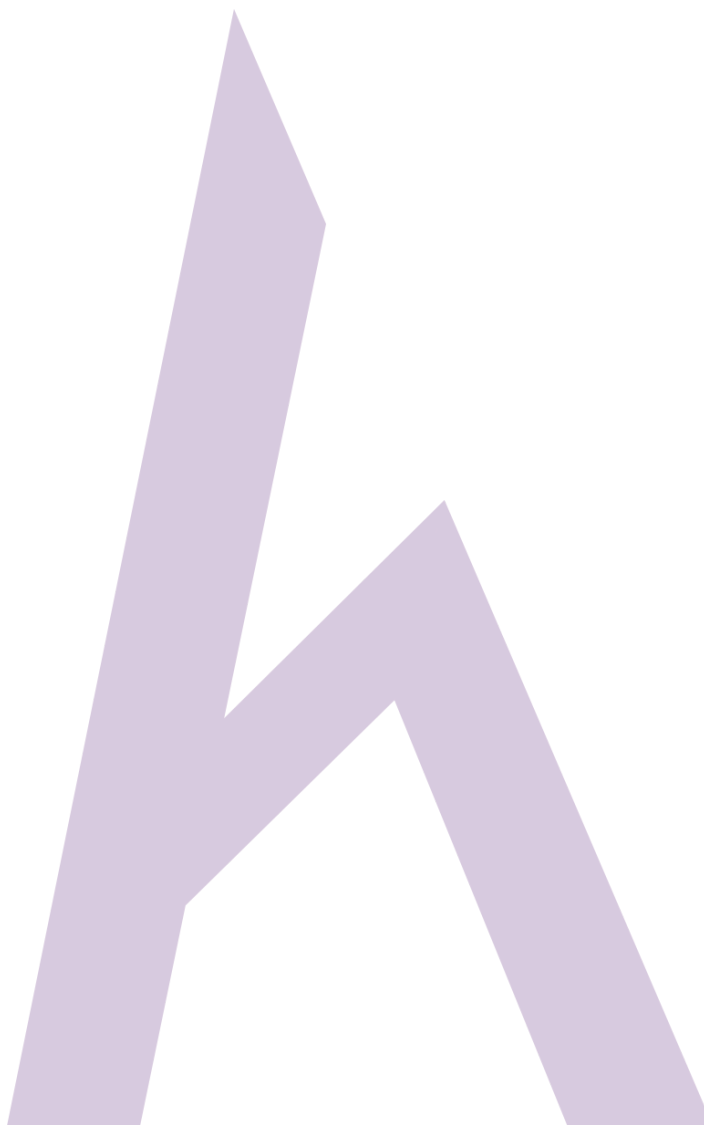


Bài: 2.4 Dấu vết & Thăm dò - Cách thăm dò dấu vết (Phần 3)

Xem bài học trên website để ủng hộ Kteam: [2.4 Dấu vết & Thăm dò - Cách thăm dò dấu vết \(Phần 3\)](#).

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage [How Kteam](#) nhé!



Cách thăm dò dấu vết

Dấu vết WHOIS (WHOIS Footprinting)

Truy tìm thông tin WHOIS (WHOIS Lookup)

“**WHOIS**” giúp thu thập thông tin về tên miền, thông tin quyền sở hữu. Địa chỉ IP, dữ liệu NetBlock, Domain Name Servers và các thông tin khác. Đăng kí **Regional Internet Registries** (RIR) duy trì việc tra cứu WHOIS giúp tìm ra ai là người đứng sau tên miền.

Hệ thống RIR được tạo ra, cuối cùng chia thành 5 loại RIRs:

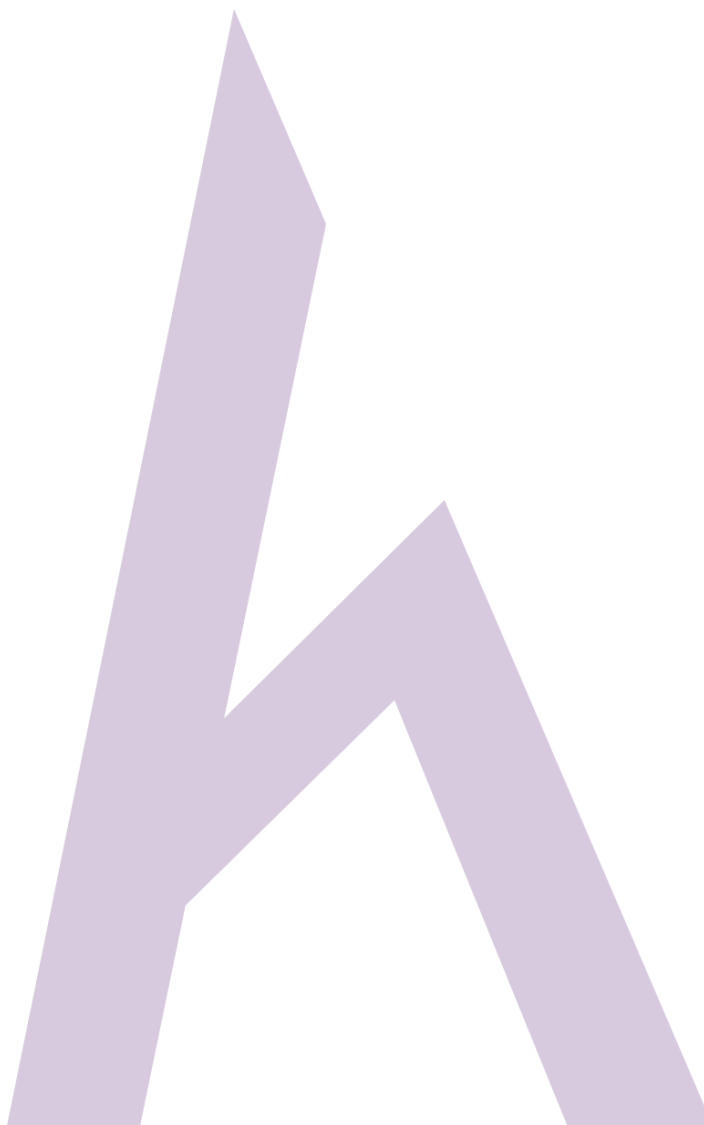
RIRs	Viết tắt	Vị trí
Trung tâm thông tin mạng Châu Phi (African Network Information Center)	AFRINIC	Châu phi
Cơ quan đăng kí số điện thoại của Mỹ (American Registry for Internet Numbers)	ARIN	Mỹ, Canada, một vài khu vực thuộc miền Caribbean, và Nam Cực
Trung tâm thông tin mạng Châu Á-Thái Bình Dương (Asia-Pacific Network Information Centre)	APNIC	Châu Á, Úc, New Zealand, và các quốc gia láng giềng
Trung tâm thông tin mạng Châu Mỹ La Tinh và Caribbean (Latin America and Caribbean Network Information Centre)	LACNIC	Châu Mỹ La Tinh và một số phần thuộc miền Caribbean
Trung tâm liên kết mạng Réseaux IP Européens	RIPE NCC	Châu Âu, Nga, Trung Đông, Trung Á

Trình diễn dấu vết WHOIS (Performing WHOIS Footprinting)

1. Truy cập URL <https://www.whois.com/>

2. Tìm kiếm miền mục tiêu

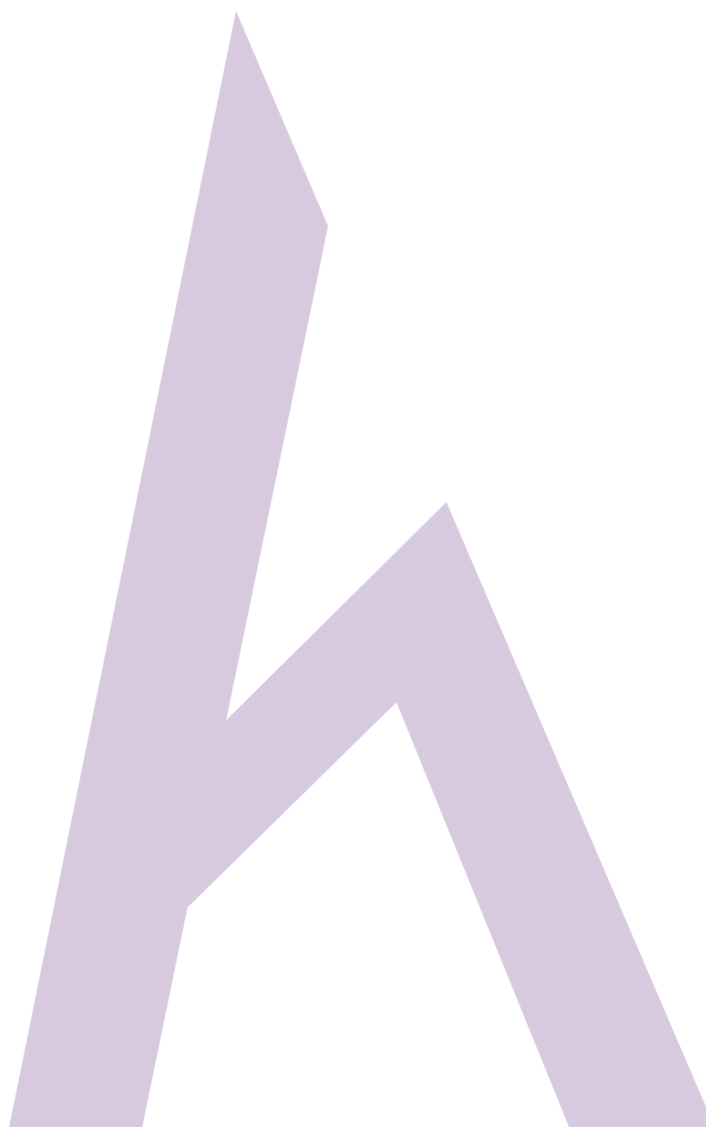
Phân tích kết quả truy tìm thông tin WHOIS



Kết quả truy tìm thông tin cho thấy hồ sơ miền hoàn chỉnh, bao gồm:

- Thông tin người đăng kí
- Thông tin tổ chức đăng kí
- Thông tin tổ chức đăng kí
- Quốc gia đăng kí
- Thông tin máy chủ tên miền
- Địa chỉ IP
- Vị trí IP
- ASN Trạng thái miền
- Lịch sử WHOIS
- Lịch sử IP
- Lịch sử nhân viên
- Lịch sử chủ thể

Nó cũng bao gồm các thông tin khác như Email và địa chỉ bưu điện của nhân viên & quản lí cùng với chi tiết liên hệ. Bạn có thể truy cập <http://whois.domaintools.com> và nhấn vào URL được nhắm tới để biết thêm thông tin tra cứu.



Bạn có thể tải xuống phần mềm : " **SmartWhois**" từ www.tamos.com cho truy tìm thông tin Whois như được thể hiện trong hình dưới đây:

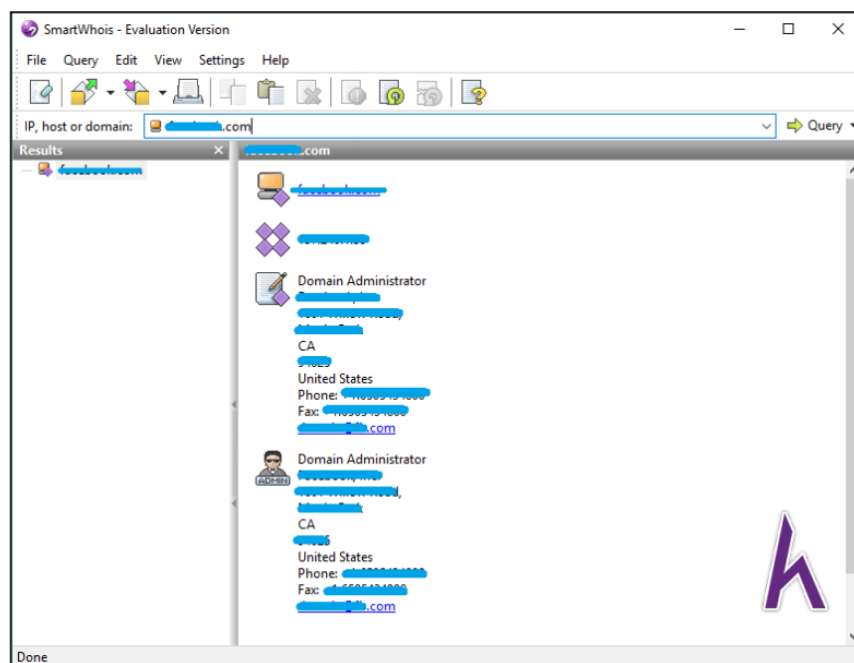
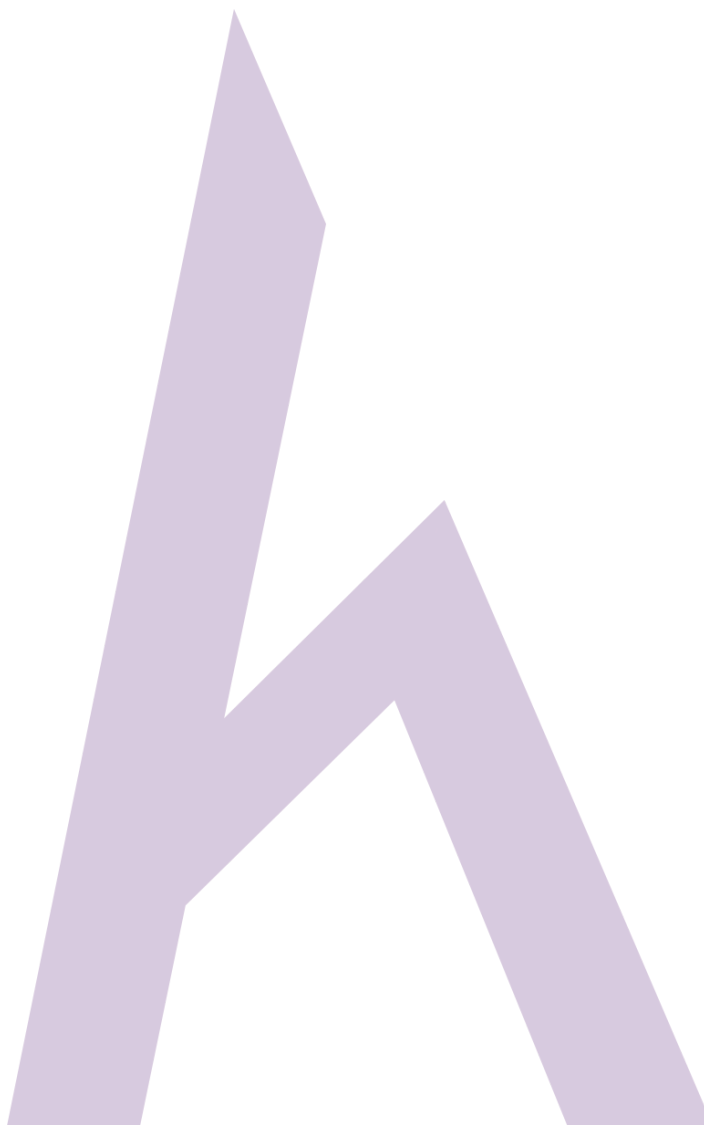


Figure 2-31 SmartWhois Lookup Application

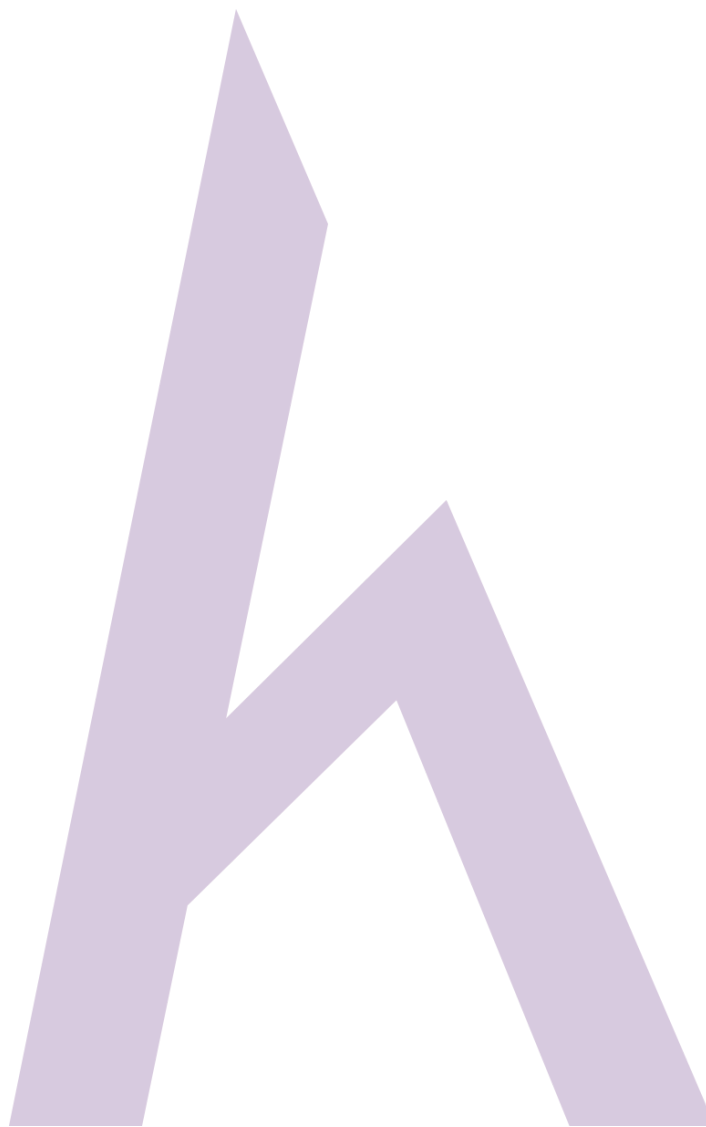
Công cụ truy tìm thông tin WHOIS (WHOIS Lookup Tools)

Những công cụ được cung cấp bởi các nhà phát triển khác nhau trên truy tìm thông tin WHOIS được liệt kê dưới đây:

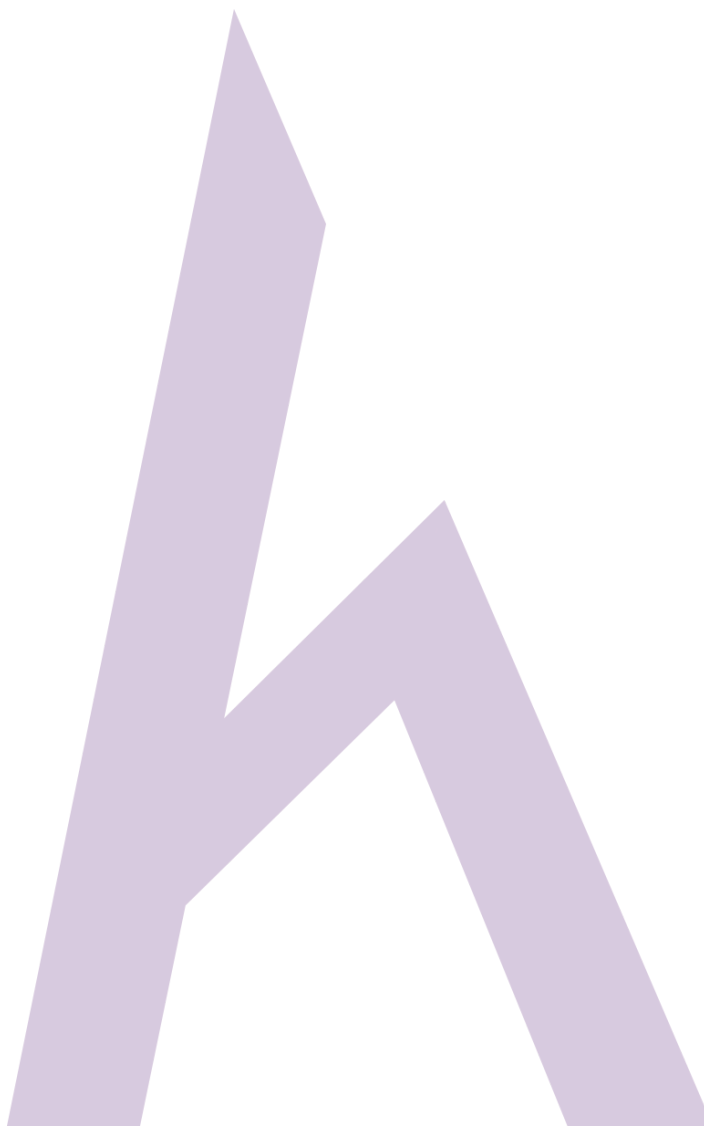
- <http://lantricks.com>
- <http://www.networkmost.com>
- <http://tialsoft.com>
- <http://www.johnru.com>
- <http://www.callerippro.com>
- <http://www.nirsoft.com>
- <http://www.sobolsoft.com>
- <http://www.softfuse.com>



Công cụ truy tìm thông tin WHOIS cho điện thoại

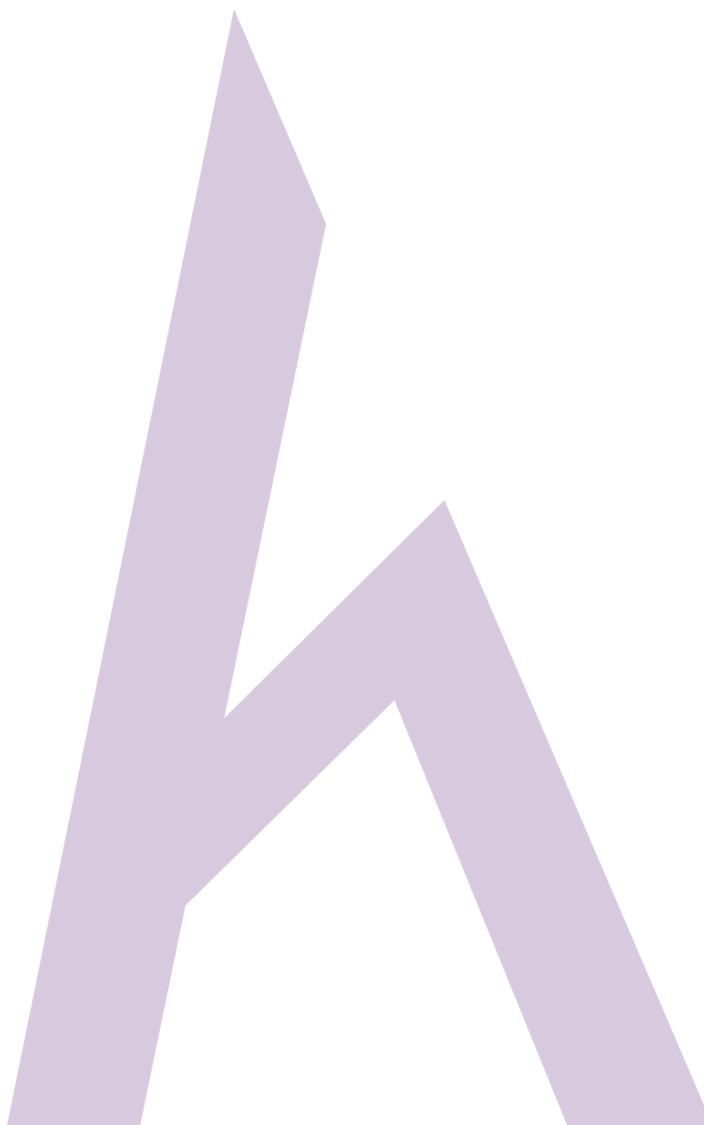


Ứng dụng “ **DNS Tools**” bởi www.dnssniffers.com có sẵn trên các cửa hàng Google Play. Nó gồm các đặc tính khác như DNS Report, Blacklist Check, Email Validation, WHOIS, lệnh ping và đảo DNS.

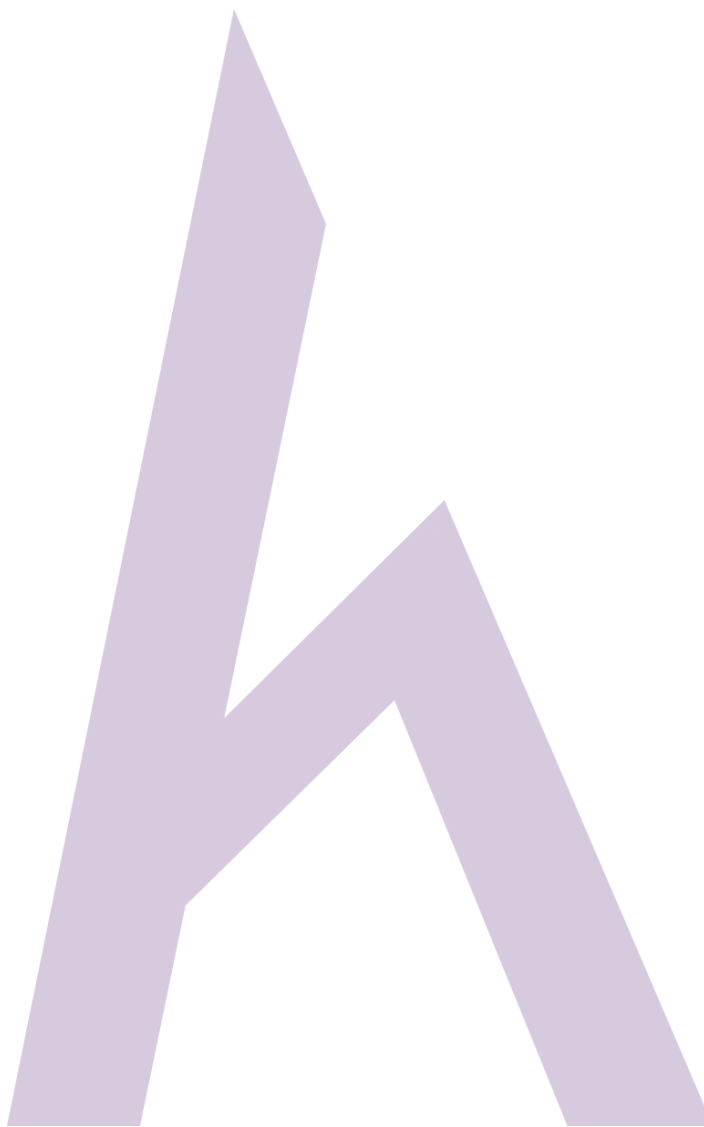


Whois bởi ứng dụng www.whois.com.au trong cửa hàng Google Play để truy tìm thông tin. Những công cụ truy tìm thông tin được cung cấp bởi www.whois.com.au như:

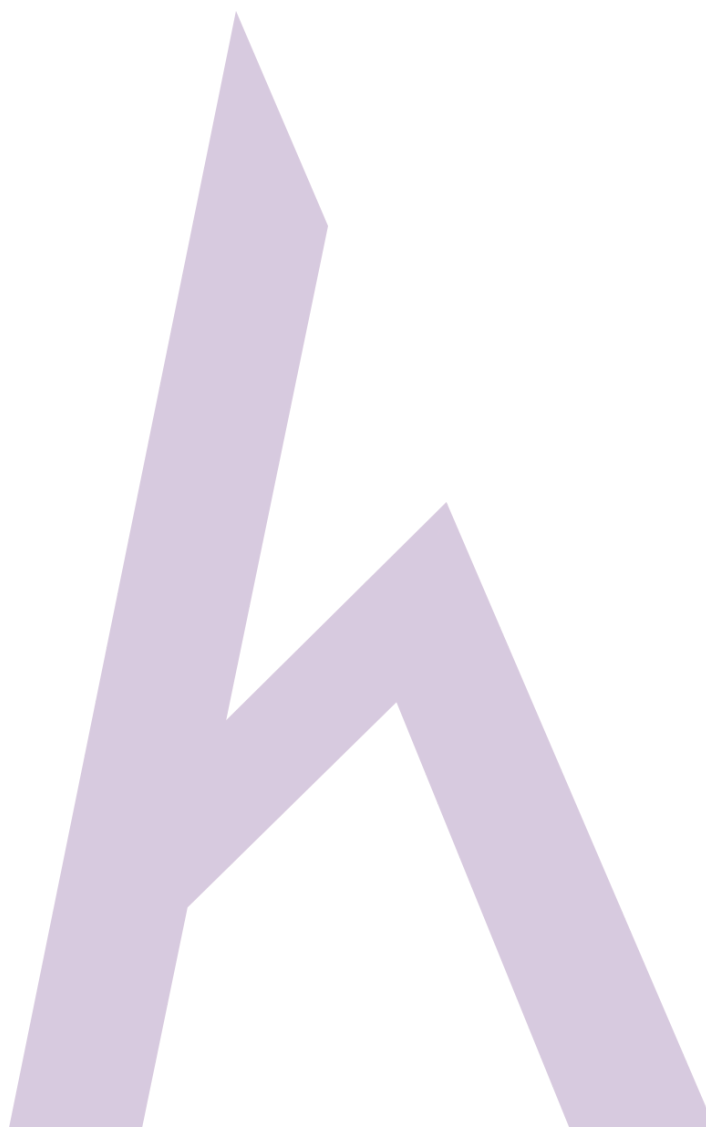
- Truy tìm thông tin WHOIS (WHOIS Lookup)
- Truy tìm thông tin DNS (DNS Lookup)
- Truy tìm thông tin RBL (RBL Lookup)
- Công cụ truy vết (Traceroute)
- Truy tìm thông tin IP (IP Lookup)
- Truy cập dữ liệu API/Bulk (API/Bulk Data Access)



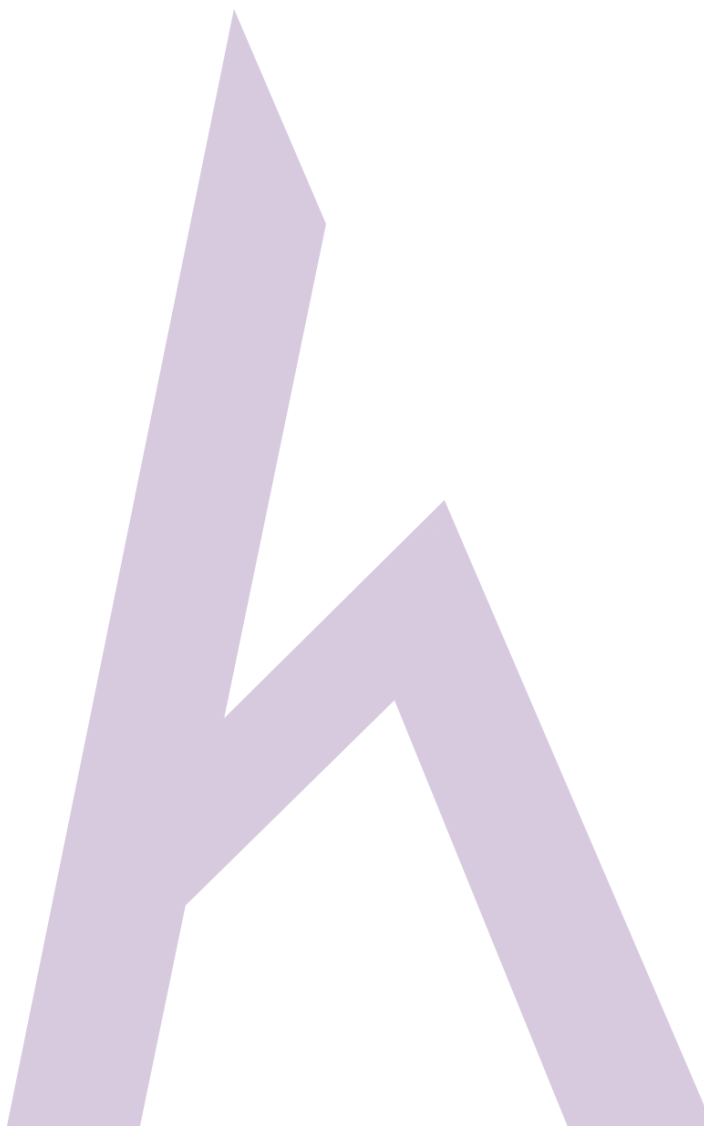
www.ultratools.com cung cấp Ultra Tools Mobile. Ứng dụng này cung cấp các đặc tính đa dạng giống như báo cáo tình trạng tên miền (Domain health report), kiểm tra tốc độ DNS (DNS Speed test), truy tìm thông tin DNS (DNS Lookup), ping và các tùy chọn khác.



Dấu vết DNS (DNS footprinting)



Thông tin truy tìm DNS là hữu ích để xác định được chủ thể trong mạng được nhắm làm mục tiêu. Nhiều công cụ sẵn có trên mạng trình diễn truy tìm thông tin DNS. Trước khi tiến hành các công cụ truy tìm thông tin DNS và kết quả tổng quan của các công cụ DNS này, bạn phải biết biểu tượng loại bản ghi và có nghĩa là:



Loại bản ghi	Mô tả
A	Địa chỉ IP của chủ thể
MX	Máy chủ thư của miền
NS	Tên máy chủ
CNAME	Việc đặt tên Canonical cho phép các bí danh đến một máy chủ
SDA	Cho biết thẩm quyền của miền
SRV	Bản tin dịch vụ
PTR	Bản đồ IP-Host
RP	Người có trách nhiệm
HINFO	Thông tin chủ thể
TXT	Bản tin không theo cấu trúc

Table 2-09 DNS Record Type

Trích thông tin DNS bằng cách sử dụng DNSStuff

Truy cập URL: <https://www.dnsstuff.com>

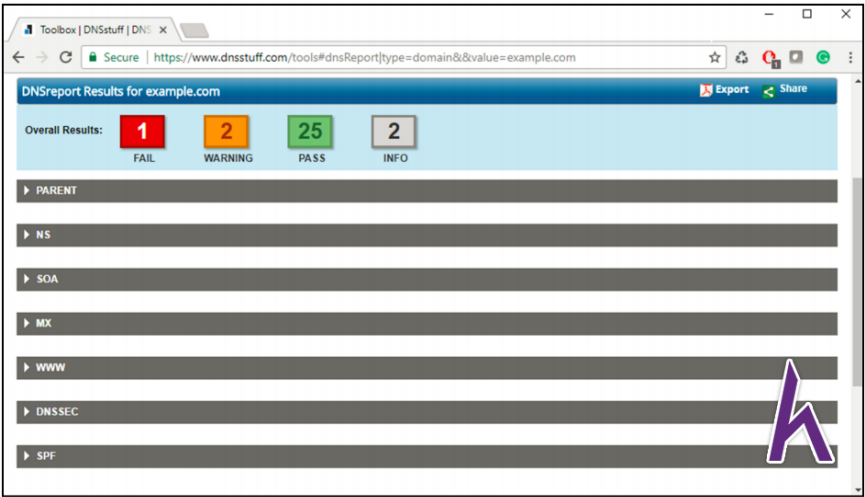
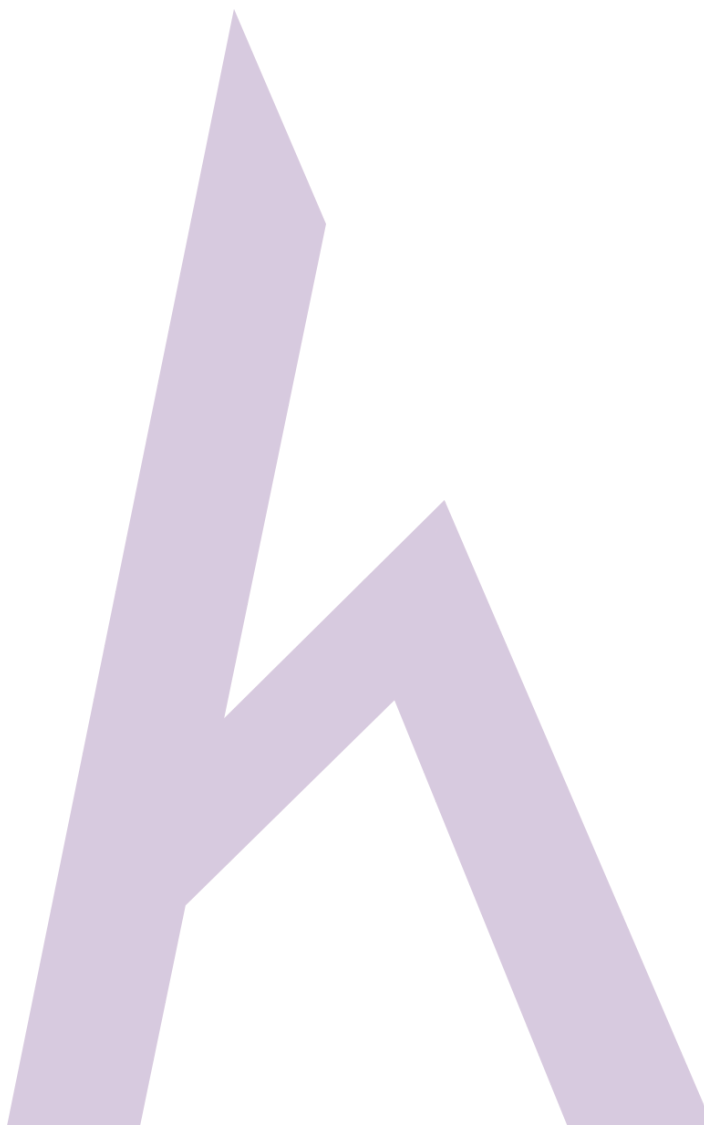
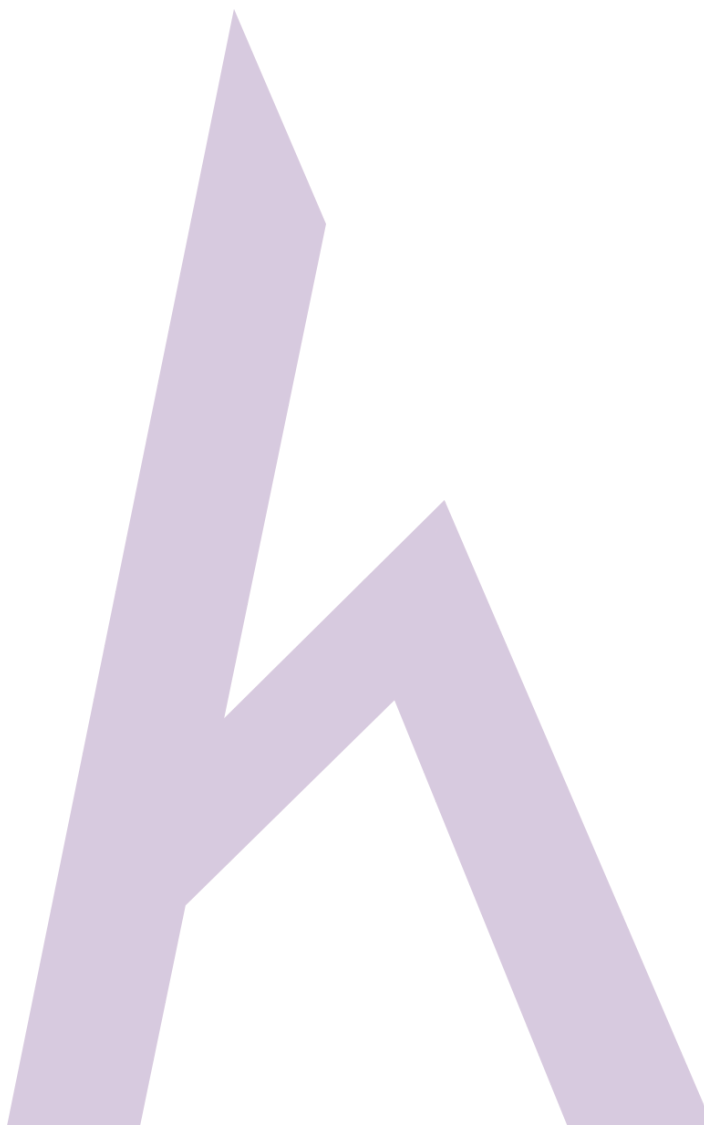


Figure 2-35 DNSStuff.com

Hình trên là đầu ra đối với [example.com](#). Bạn có thể mở rộng các trường để trích xuất thông tin.

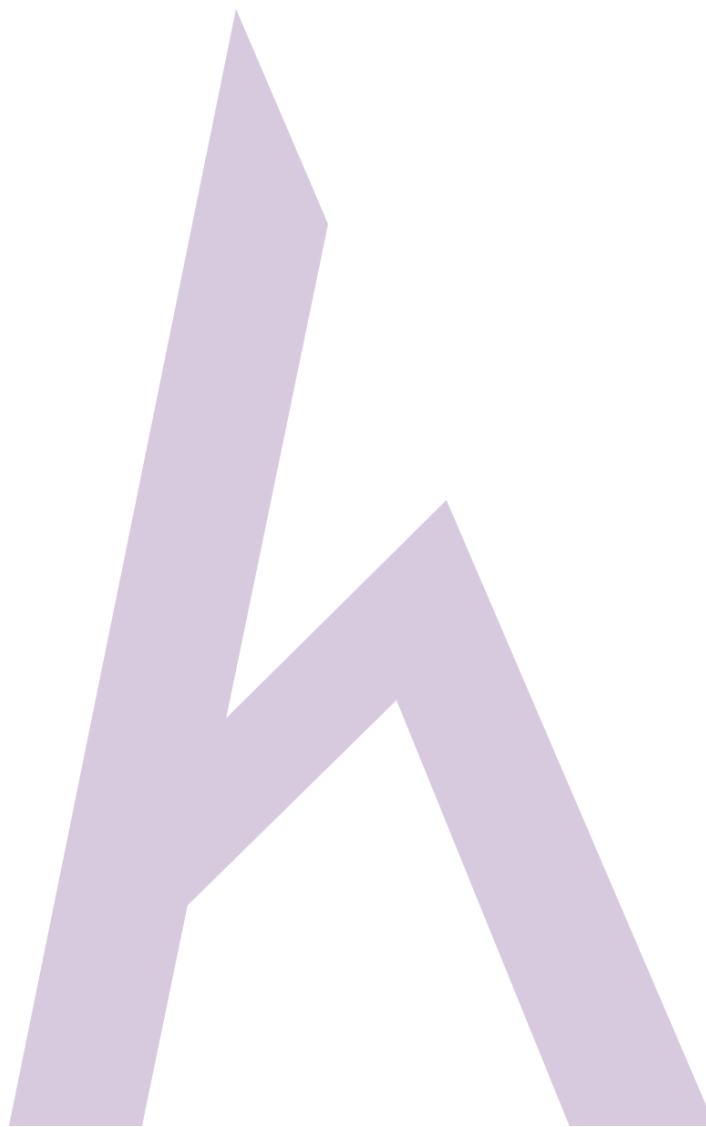


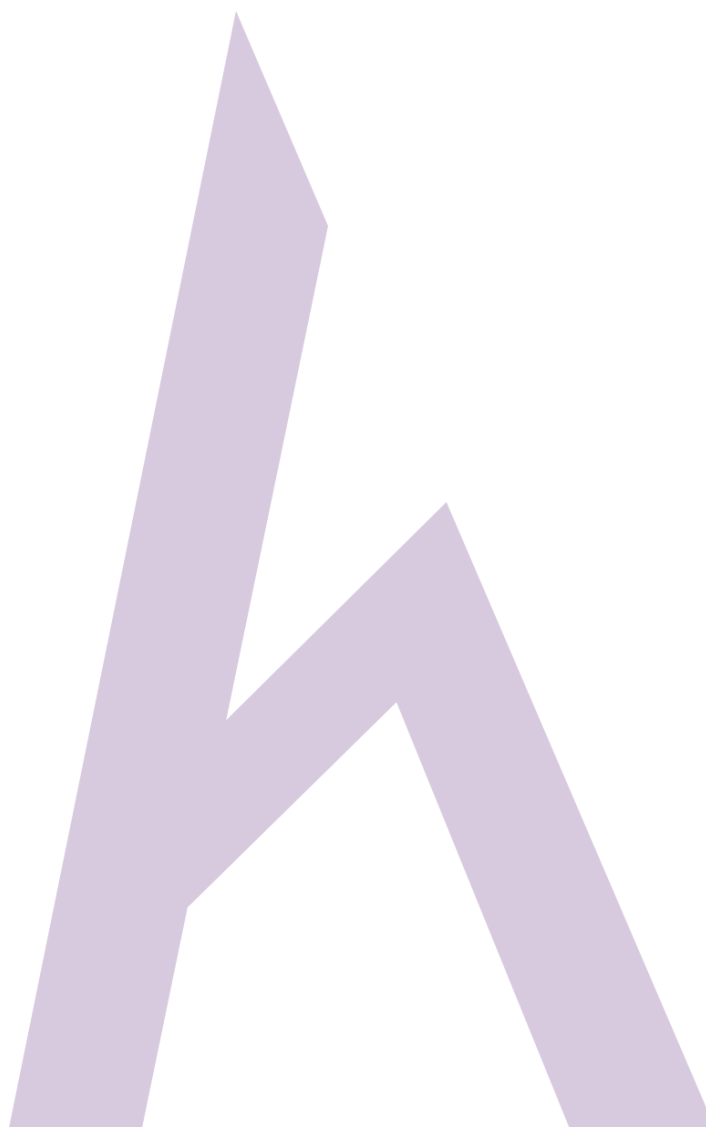
Như được hiển thị trong đầu ra sau, bạn có thể mở rộng các trường mong muốn để có được chi tiết thông tin như hình dưới đây:



Trích xuất thông tin DNS bằng cách sử dụng Domain Dossier

Truy cập trang web <https://centralops.net/co/> và nhập địa chỉ IP của Miền bạn muốn tìm kiếm.

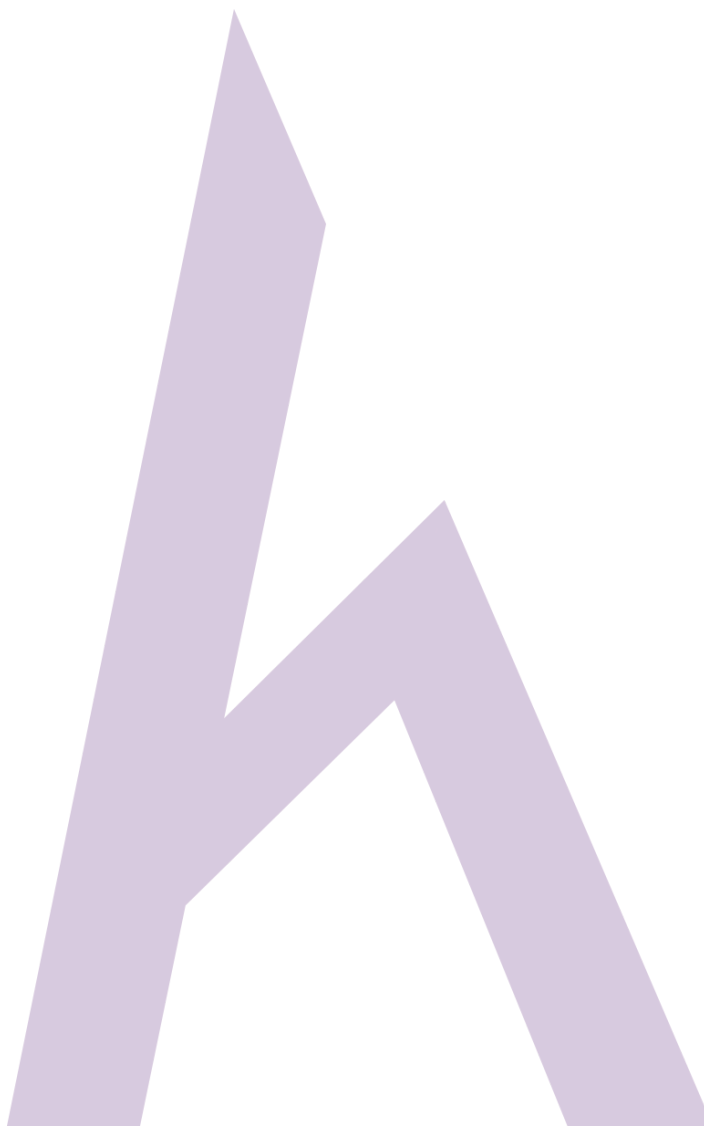




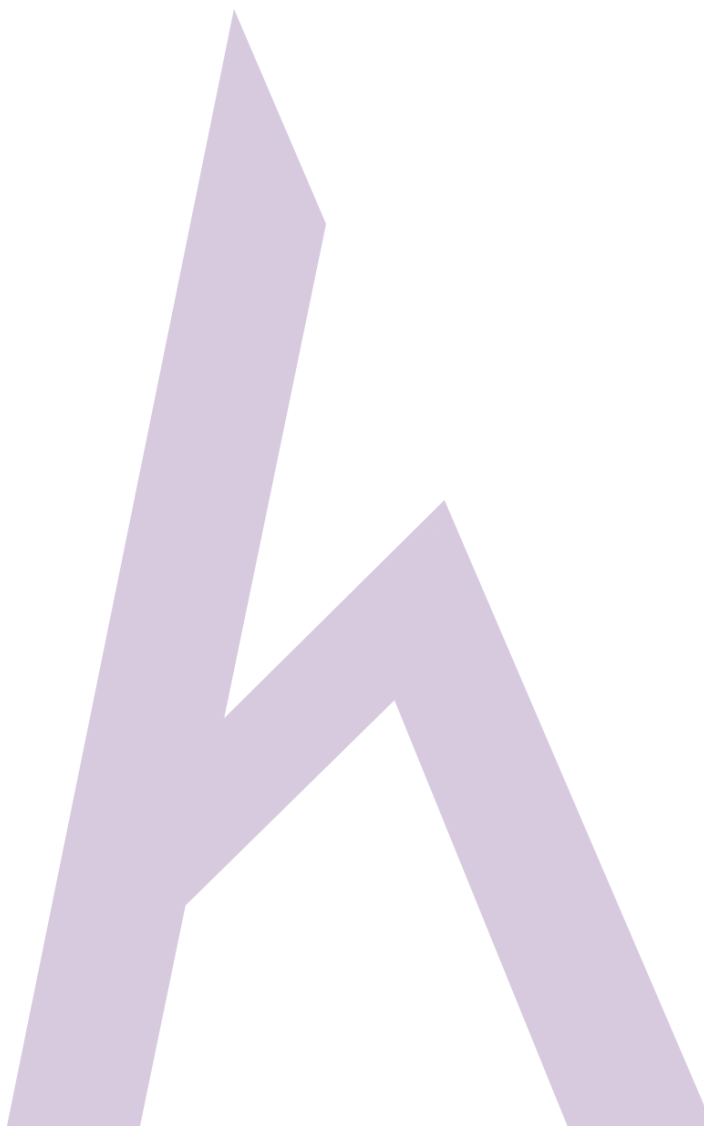
Kết quả mang lại tên chuẩn, bí danh, địa chỉ IP, bản ghi tên whois, bản ghi whois mạng và bản ghi DNS. Hãy xem xét hình bên dưới.

Công cụ thăm vấn DNS (DNS Interrogation Tools)

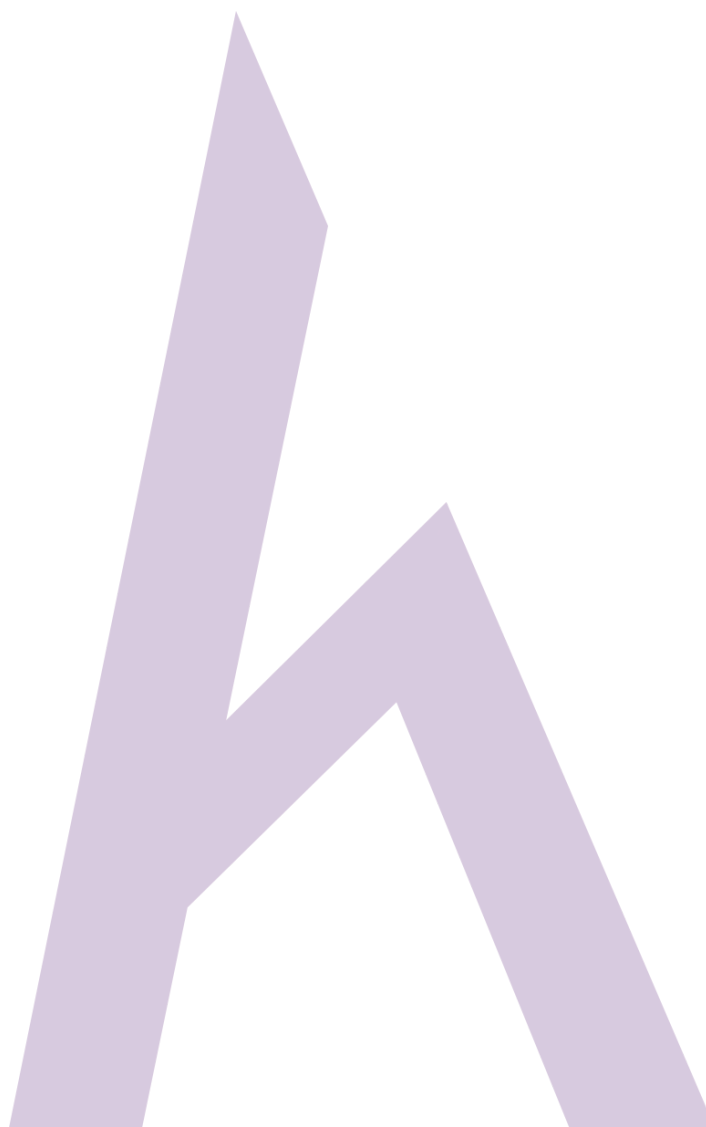
Có nhiều công cụ trực tuyến có sẵn cho thông tin truy tìm DNS, một vài công cụ đó được liệt kê danh sách dưới đây:



- <http://www.dnsstuff.com>
- <http://network-tools.com>
- <http://www.kloth.net>
- <http://www.dnswatch.info>
- <http://www.domaintools.com>
- <http://www.ultratools.com>
- <http://www.webmaster-toolkit.com>
- <http://www.mydnstools.info>
- <http://www.nirdoft.net>

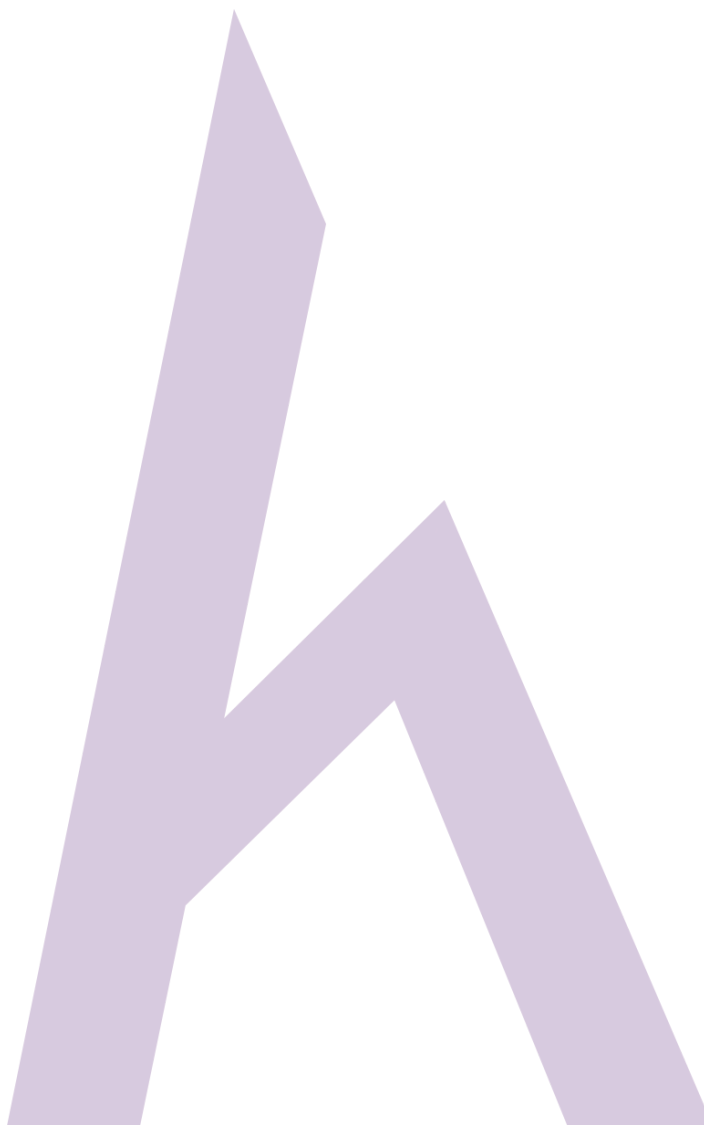


Dấu vết mạng



Một trong những kiểu dấu vết quan trọng đó là **dấu vết mạng**. May thay, có nhiều công cụ có sẵn có thể được sử dụng cho dấu vết mạng để thu thập thông tin về mạng được chọn làm mục tiêu. Sử dụng những công cụ này, người tìm kiếm thông tin có thể sáng tạo bản đồ mạng mục tiêu. Tương tự, bằng cách này bạn có thể trích thông tin như:

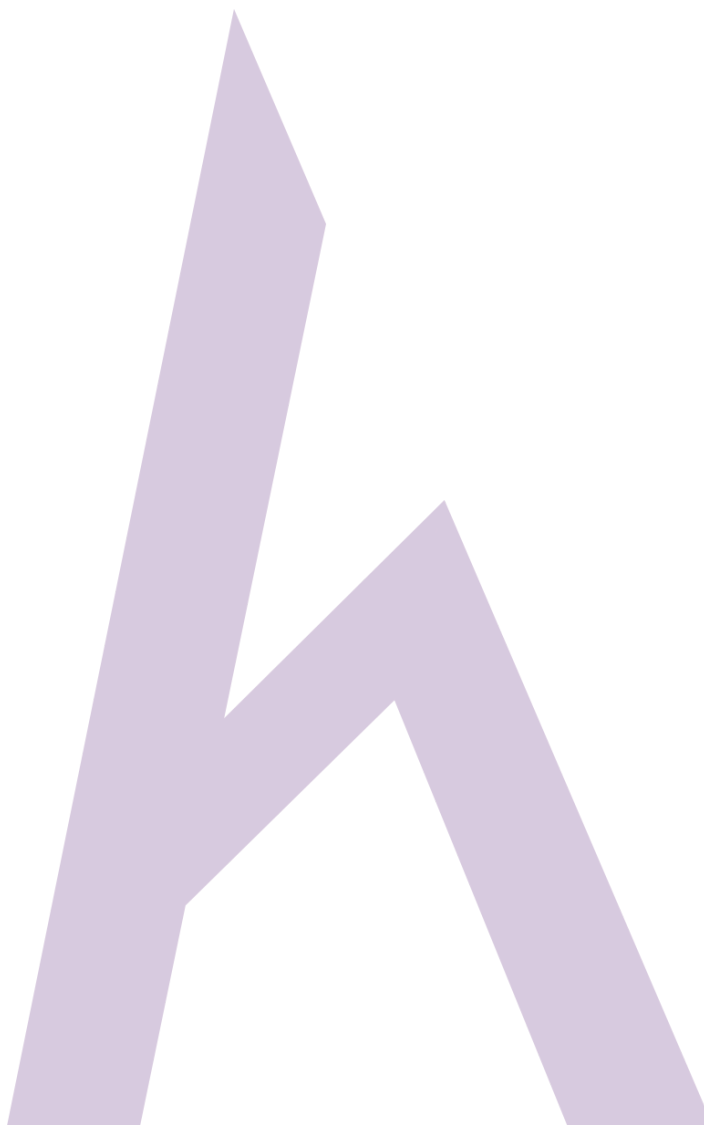
- Miền địa chỉ mạng
- Tên máy chủ
- Máy chủ bị lộ
- Thông tin bản ứng dụng và OS
- Trạng thái bản vá của máy chủ và ứng dụng
- Cấu trúc của ứng dụng và máy chủ back-end



Công cụ cho những mục đích này được liệt kê phía dưới :

- Whois
- Ping
- Nslookup
- Tracert

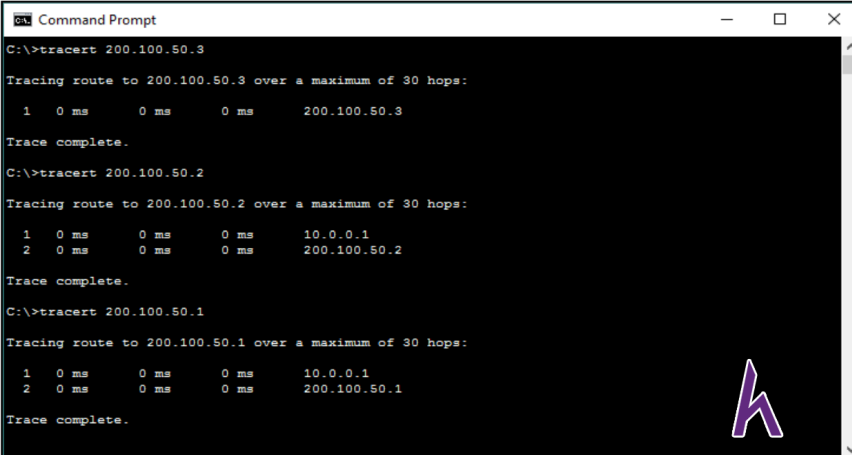
Lệnh Traceroute



Những tùy chọn lệnh **Tracert** có sẵn trong tất cả các hệ thống điều hành cũng như đặc tính năng dòng lệnh. **Traceroute** đồ quan, đồ họa và những ứng dụng Traceroute dựa trên GUI đều có sẵn. **Traceroute** và kết quả lệnh **Tracert** trong thông tin bản vá từ nguồn đến đích theo kiểu nhảy. Kết quả bao gồm tất cả các nhịp nhảy giữa các nguồn đến đích. Kết quả cũng cho thấy các góc trễ giữa các nhịp nhảy.

Phân tích Traceroute

Chú ý ví dụ sau, nơi mà kẻ tấn công đang cố gắng để chiếm được thông tin mạng bằng cách sử dụng lệnh `tracert`. Sau khi quan sát kết quả dưới đây, bạn có thể xác định được bản đồ mạng.



```
Command Prompt
C:\>tracert 200.100.50.3

Tracing route to 200.100.50.3 over a maximum of 30 hops:
  1  0 ms    0 ms    0 ms    200.100.50.3
Trace complete.

C:\>tracert 200.100.50.2

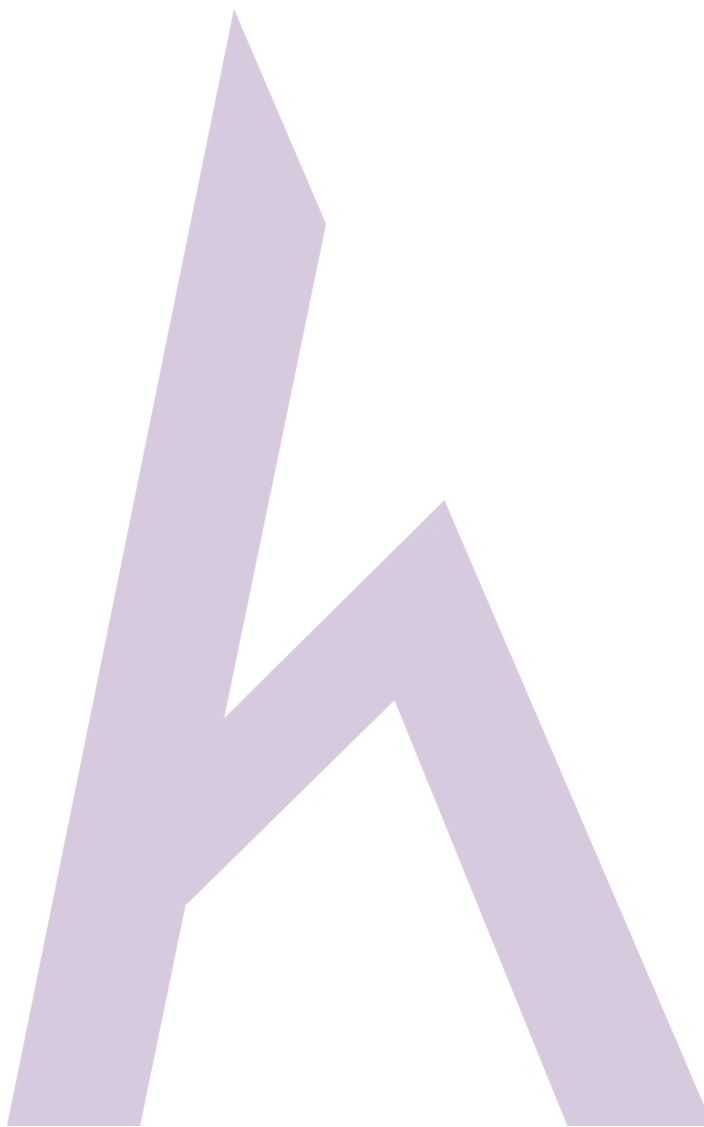
Tracing route to 200.100.50.2 over a maximum of 30 hops:
  1  0 ms    0 ms    0 ms    10.0.0.1
  2  0 ms    0 ms    0 ms    200.100.50.2
Trace complete.

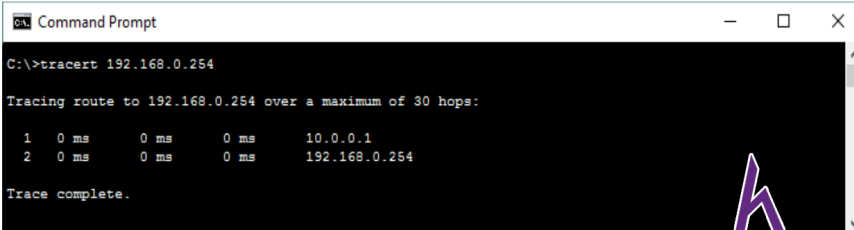
C:\>tracert 200.100.50.1

Tracing route to 200.100.50.1 over a maximum of 30 hops:
  1  0 ms    0 ms    0 ms    10.0.0.1
  2  0 ms    0 ms    0 ms    200.100.50.1
Trace complete.
```

Figure 2-39 Tracert

10.0.0.1 là hop đầu tiên, có nghĩa là nó là gateway. Kết quả Tracert **200.100.50.3** hiển thị, **200.100.50.3** là một giao diện khác của thiết bị hop đầu tiên trong khi IP được kết nối bao gồm **200.100.50.2** & **200.100.50.1**.





The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command entered is `C:\>tracert 192.168.0.254`. The output shows the tracing route to 192.168.0.254 over a maximum of 30 hops. The route consists of two hops: Hop 1 from 10.0.0.1 to 10.0.0.1 with 0 ms latency, and Hop 2 from 10.0.0.1 to 192.168.0.254 with 0 ms latency. The trace is complete. A small purple 'h' logo is visible in the bottom right corner of the command prompt window.

```
Command Prompt
C:\>tracert 192.168.0.254

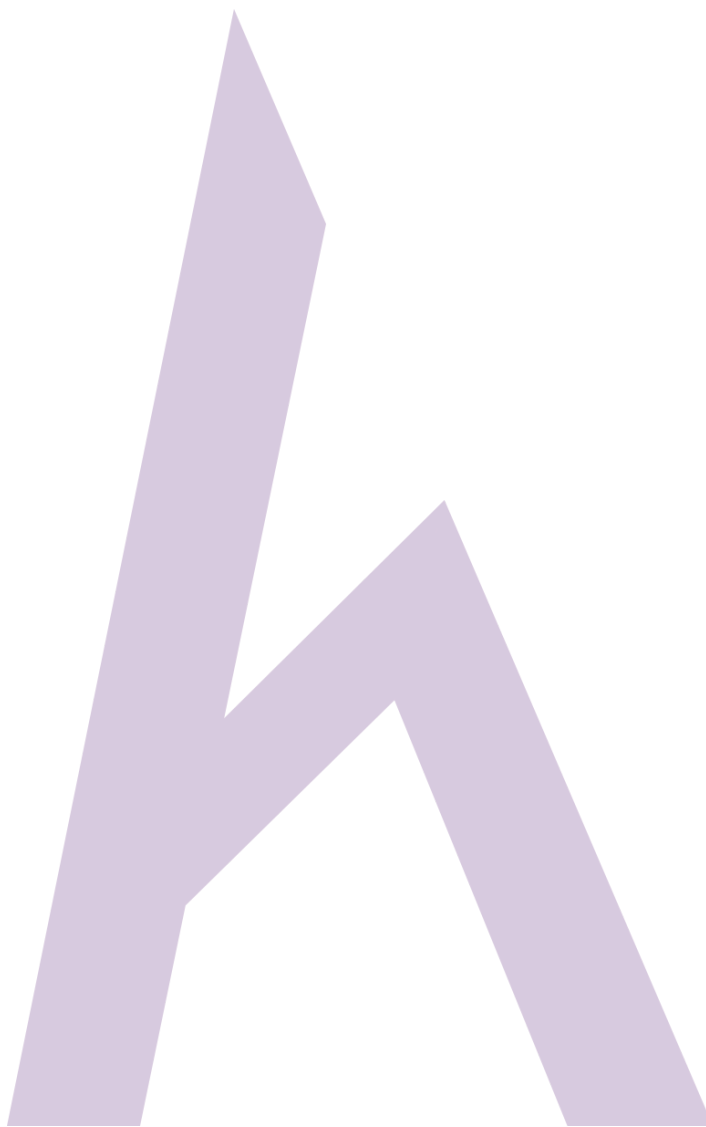
Tracing route to 192.168.0.254 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    10.0.0.1
  2  0 ms    0 ms    0 ms    192.168.0.254

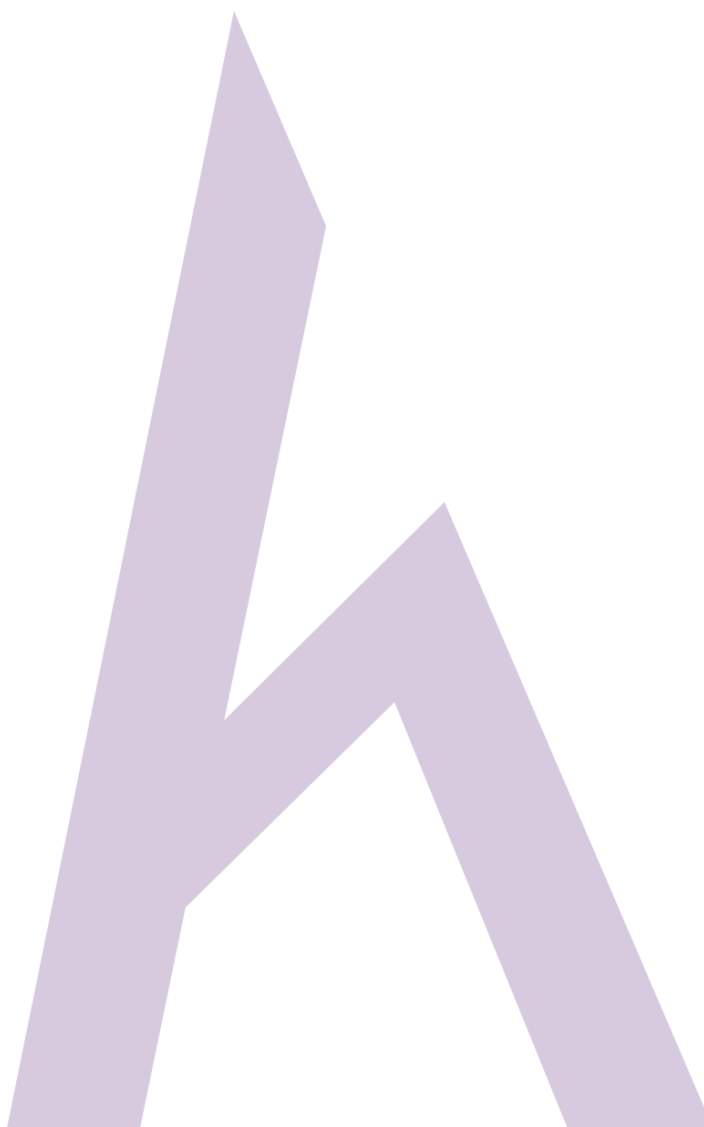
Trace complete.
```

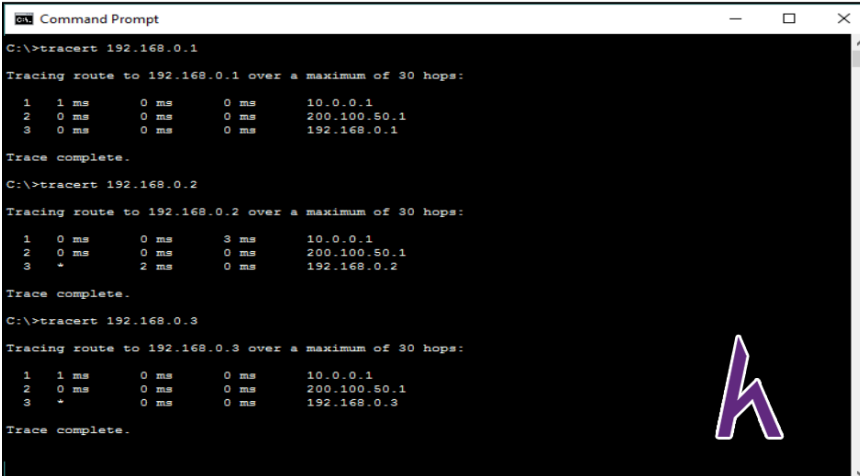
Figure 2-40 Tracert

192.168.0.254 nằm cạnh hop cuối cùng **10.0.0.1**. Nó có thể được kết nối với **200.100.50.1** hoặc



200.100.50.2. Để xác minh, hãy theo dõi tuyến đường tiếp theo.





```
Command Prompt
C:\>tracert 192.168.0.1

Tracing route to 192.168.0.1 over a maximum of 30 hops:

  1  1 ms    0 ms    0 ms    10.0.0.1
  2  0 ms    0 ms    0 ms    200.100.50.1
  3  0 ms    0 ms    0 ms    192.168.0.1

Trace complete.

C:\>tracert 192.168.0.2

Tracing route to 192.168.0.2 over a maximum of 30 hops:

  1  0 ms    0 ms    3 ms    10.0.0.1
  2  0 ms    0 ms    0 ms    200.100.50.1
  3  *        2 ms    0 ms    192.168.0.2

Trace complete.

C:\>tracert 192.168.0.3

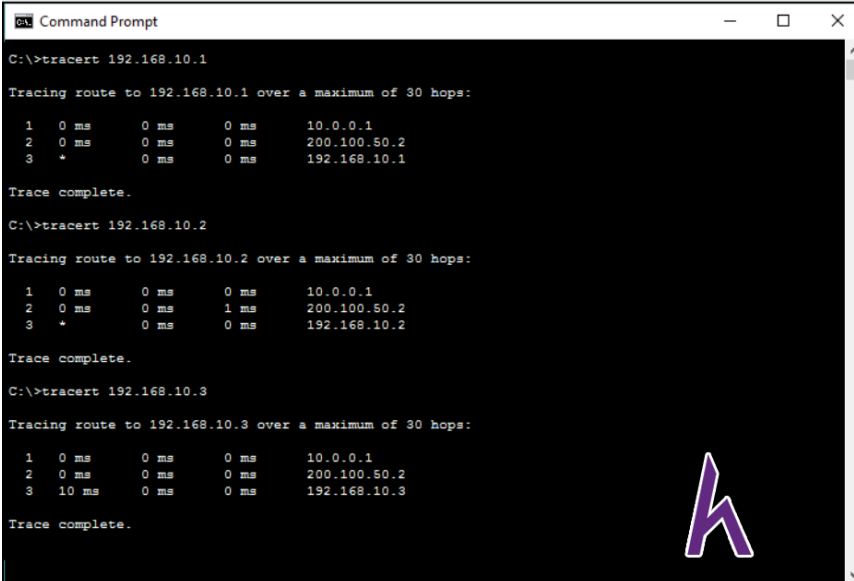
Tracing route to 192.168.0.3 over a maximum of 30 hops:

  1  1 ms    0 ms    0 ms    10.0.0.1
  2  0 ms    0 ms    0 ms    200.100.50.1
  3  *        0 ms    0 ms    192.168.0.3

Trace complete.
```

Figure 2-41 Tracert

192.168.0.254 là một giao diện khác của thiết bị mạng, tức là **200.100.50.1** được kết nối bên cạnh **10.0.0.1**. **192.168.0.1**, **192.168.0.2** & **192.168.0.3** được kết nối trực tiếp với **192.168.0.254**.



```

Command Prompt

C:\>tracert 192.168.10.1

Tracing route to 192.168.10.1 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    10.0.0.1
  2  0 ms    0 ms    0 ms    200.100.50.2
  3  *        0 ms    0 ms    192.168.10.1

Trace complete.

C:\>tracert 192.168.10.2

Tracing route to 192.168.10.2 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    10.0.0.1
  2  0 ms    0 ms    1 ms    200.100.50.2
  3  *        0 ms    0 ms    192.168.10.2

Trace complete.

C:\>tracert 192.168.10.3

Tracing route to 192.168.10.3 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    10.0.0.1
  2  0 ms    0 ms    0 ms    200.100.50.2
  3  10 ms   0 ms    0 ms    192.168.10.3

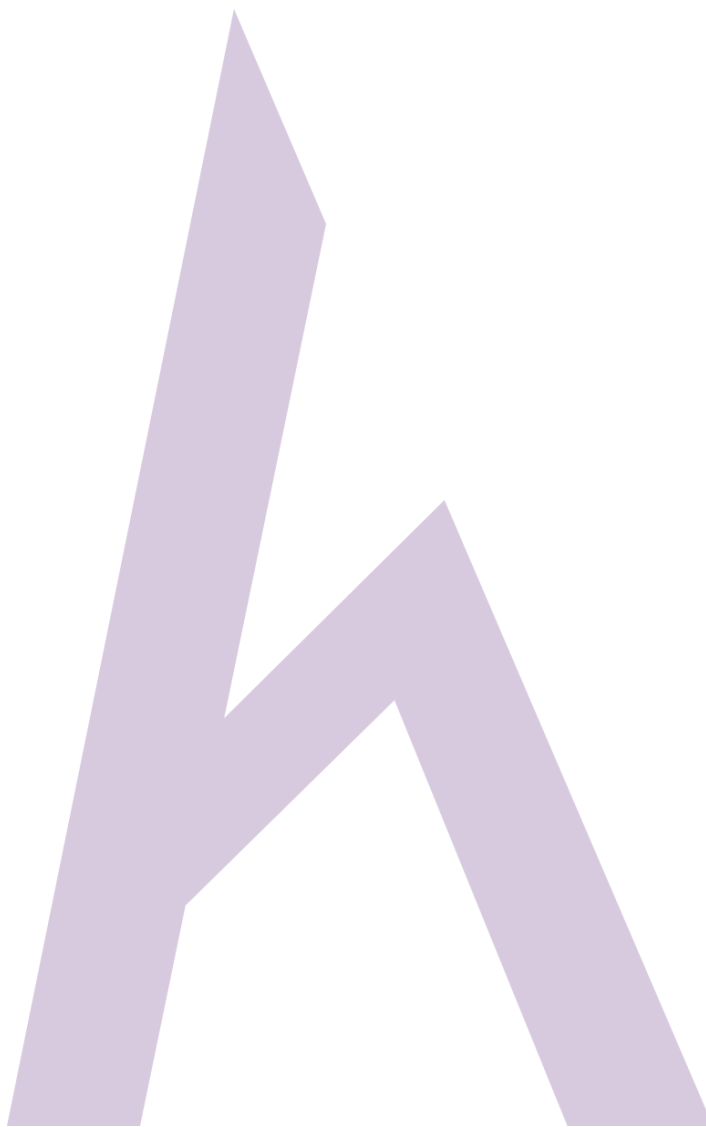
Trace complete.

```

Figure 2-42 Tracert

192.168.10.254 là một giao diện khác của thiết bị mạng, tức là **200.100.50.2** được kết nối tiếp theo **10.0.0.1**. **192.168.10.1**, **192.168.10.2** & **192.168.10.3** được kết nối trực tiếp với **192.168.10.254**.

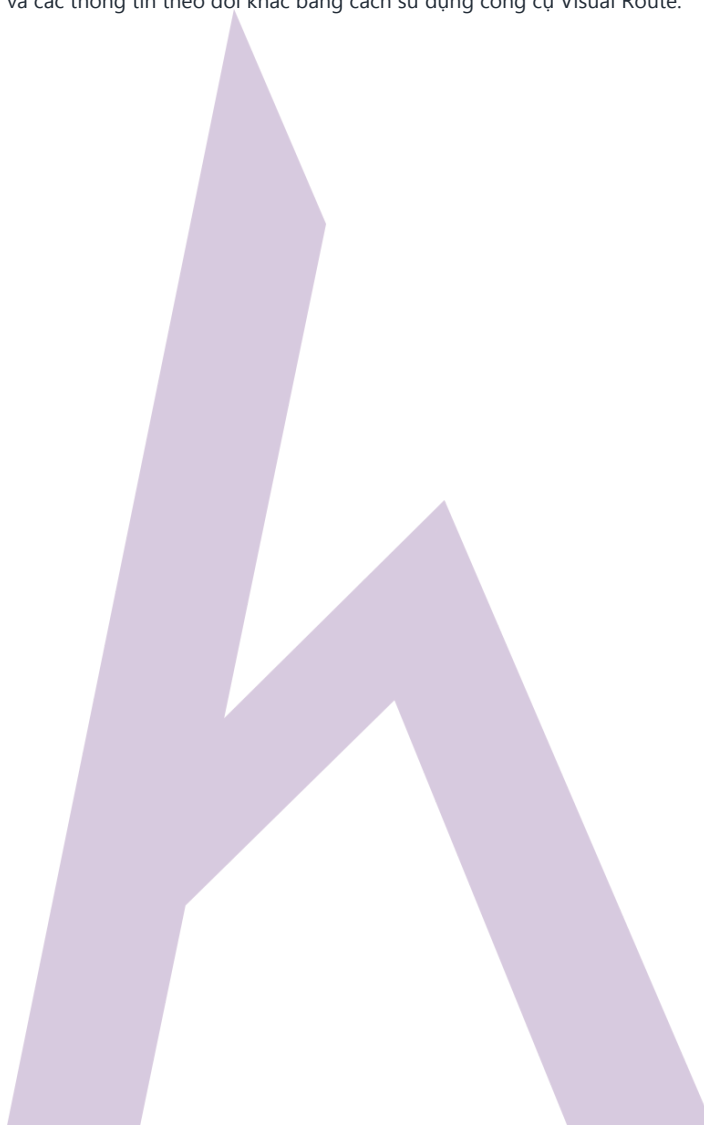
Công cụ Traceroute

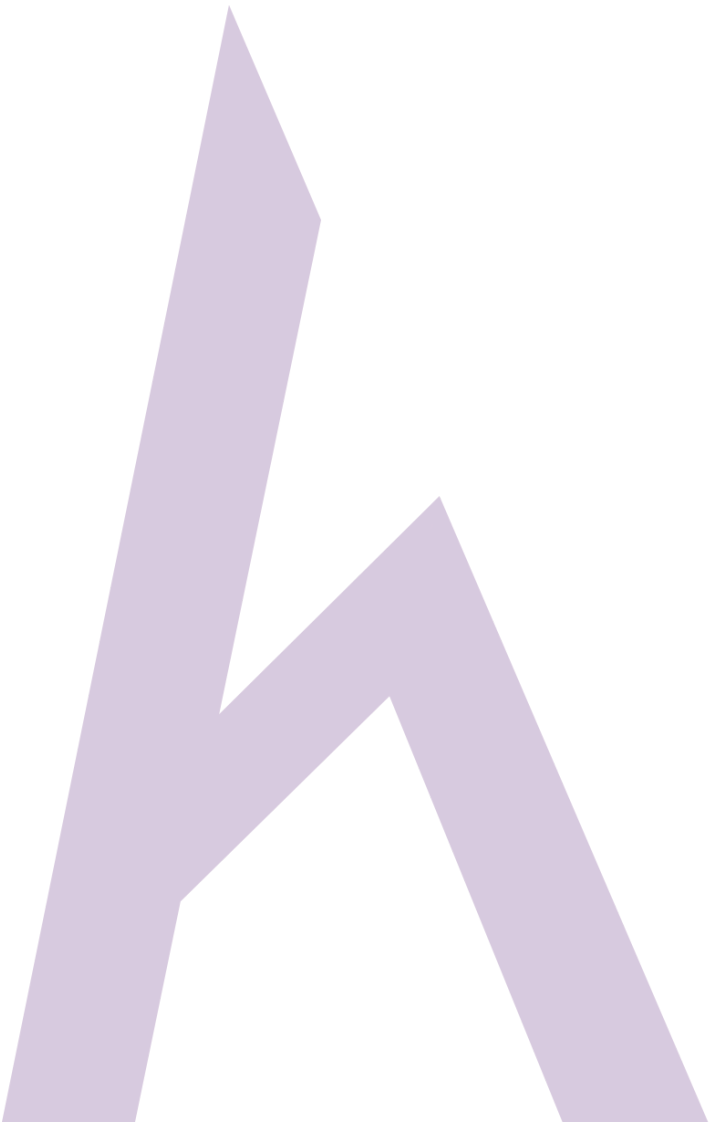


Traceroute Tools	Website
Path Analyzer Pro	www.pathanalyzer.com
Visual Route	www.visualroute.com
Troute	www.mcafee.com
3D Traceroute	www.d3tr.de



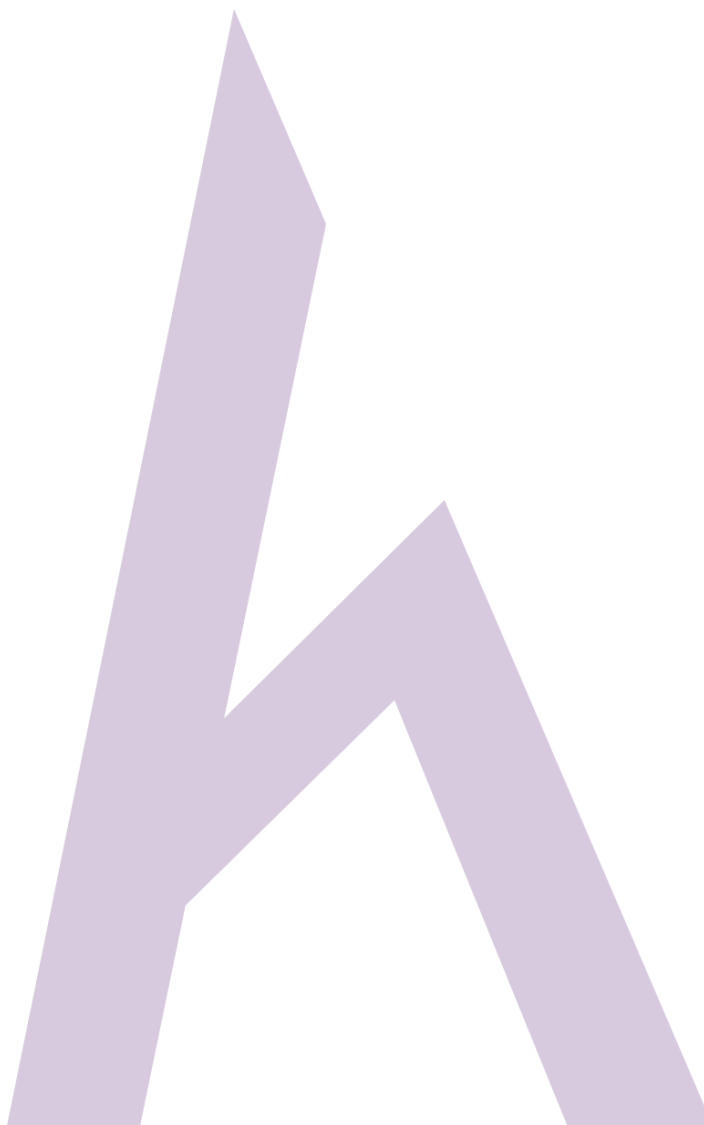
Hình ảnh dưới đây chỉ rõ tầm nhìn địa lý và các thông tin theo dõi khác bằng cách sử dụng công cụ Visual Route.



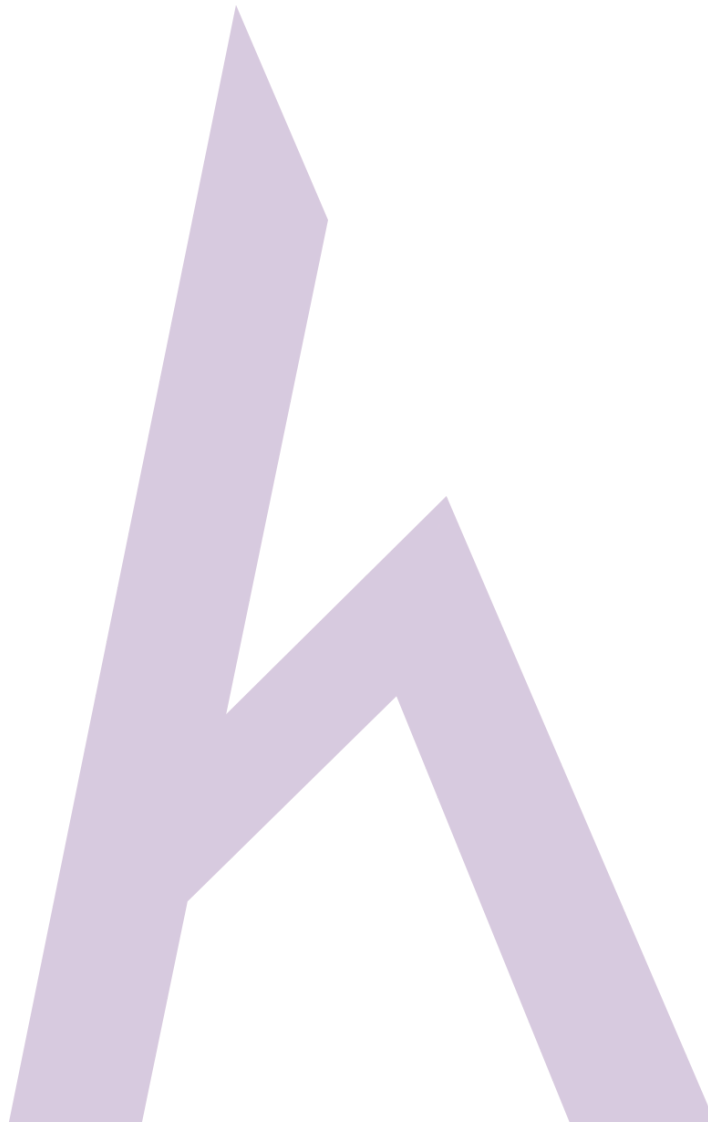


Thăm dò dấu vết thông qua kỹ thuật xã hội

Trong dấu vết, một trong những yếu tố dễ nhất để hack là con người. Chúng ta có thể thu thập thông tin từ một con người khá dễ dàng hơn là lấy thông tin từ các hệ thống. Bằng cách sử dụng kỹ thuật xã hội, một số kỹ thuật kỹ thuật xã hội cơ bản như:

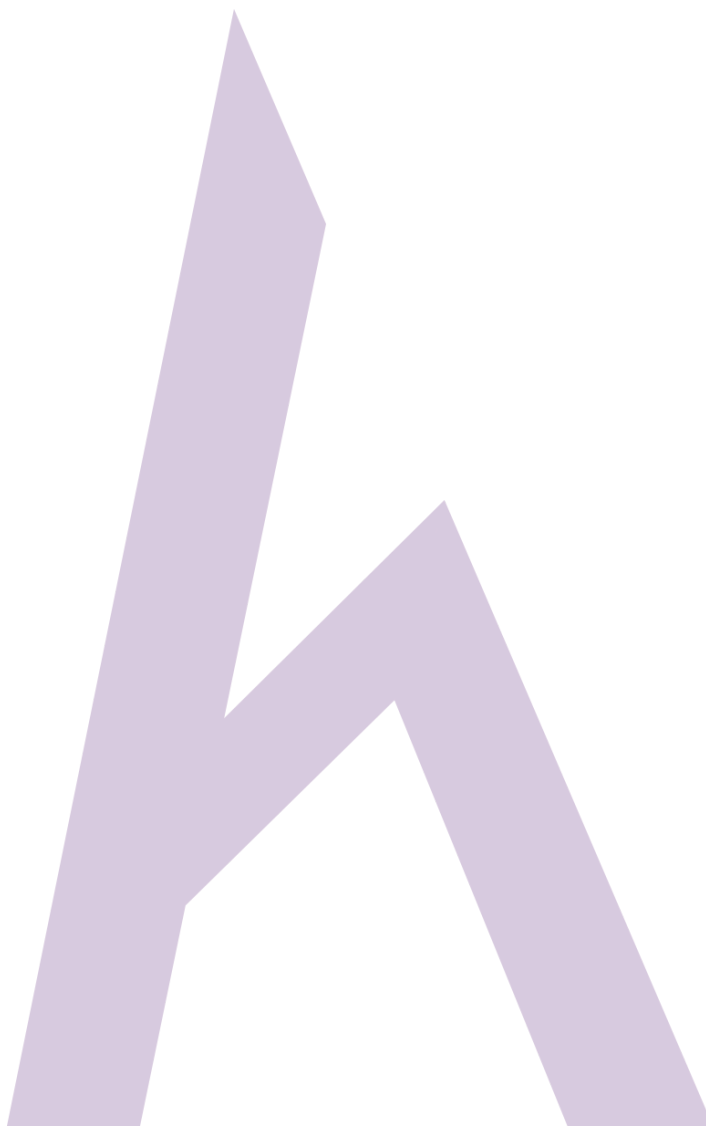


- Shoulder Surfing
- Dumpster Diving
- Mạo danh (Impersonation)

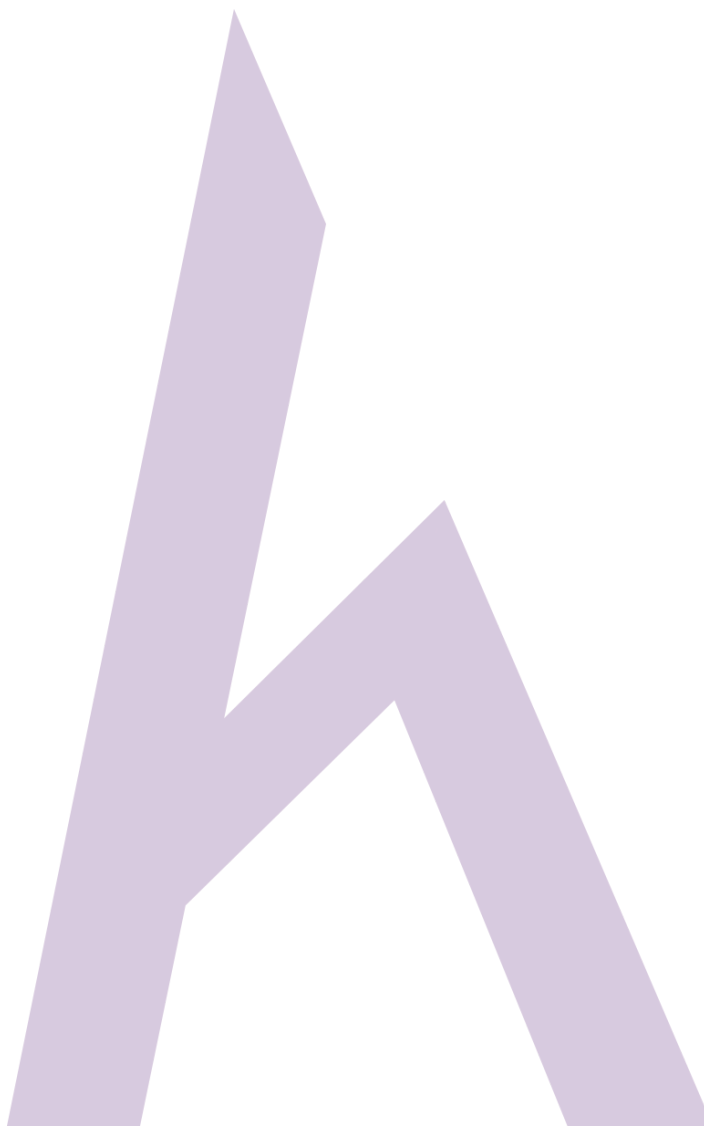


- Nghe trộm (Eavesdropping)

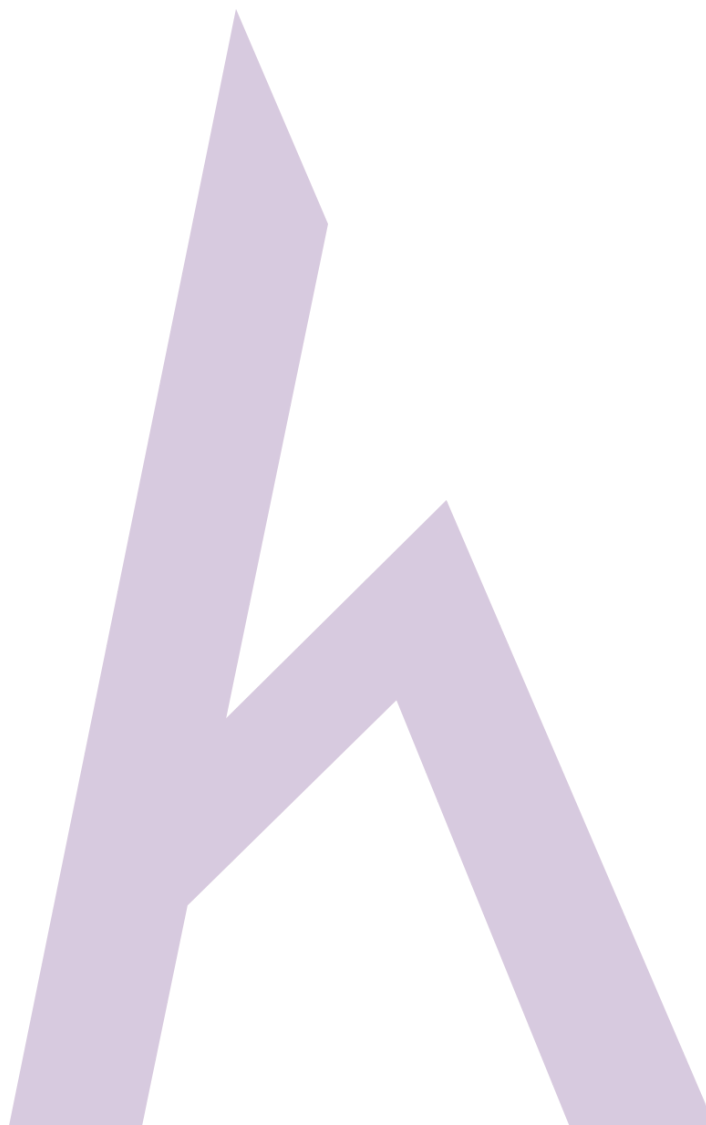
Kỹ thuật xã hội (Social Engineering)



Bạn có thể hiểu **Social Engineering** (kỹ thuật xã hội) như một nghệ thuật trích xuất thông tin nhạy cảm từ con người. Kỹ sư xã hội giữ mình không bị phát hiện, mọi người không hay biết và bất cẩn đã chia sẻ thông tin giá trị của họ. Thông tin này có liên quan đến loại kỹ thuật xã hội. Trong khía cạnh bảo mật thông tin, **Footprinting** thông qua xã hội kỹ thuật thu thập thông tin như:



- Thông tin thẻ tín dụng
- Tên đăng nhập và mật khẩu
- Thông tin công nghệ và thiết bị bảo mật
- Thông tin hệ điều hành
- Thông tin phần mềm
- Thông tin mạng
- Thông tin địa chỉ IP và máy chủ định danh.



Nghe trộm (Eavesdropping)

Eavesdropping (nghe trộm) là một loại kỹ thuật xã hội, trong đó kỹ sư xã hội sẽ tập hợp thông tin bằng cách nghe cuộc trò chuyện bí mật. Điều này diễn ra bao gồm nghe, đọc hoặc truy cập bất kỳ nguồn thông tin nào mà không được thông báo.

Lừa đảo (Phishing)

Trong quy trình **Phishing**, Email được gửi đến một nhóm được nhắm làm mục tiêu chứa nội dung thư email trông hợp pháp.

Người nhận nhấp vào liên kết được đề cập trong email giả sử liên kết đó là liên kết hợp pháp. Khi người đọc nhấp vào liên kết, dễ bị dụ dỗ để cung cấp thông tin. Nó chuyển hướng người dùng đến trang web giả mạo giống như trang web chính thức.

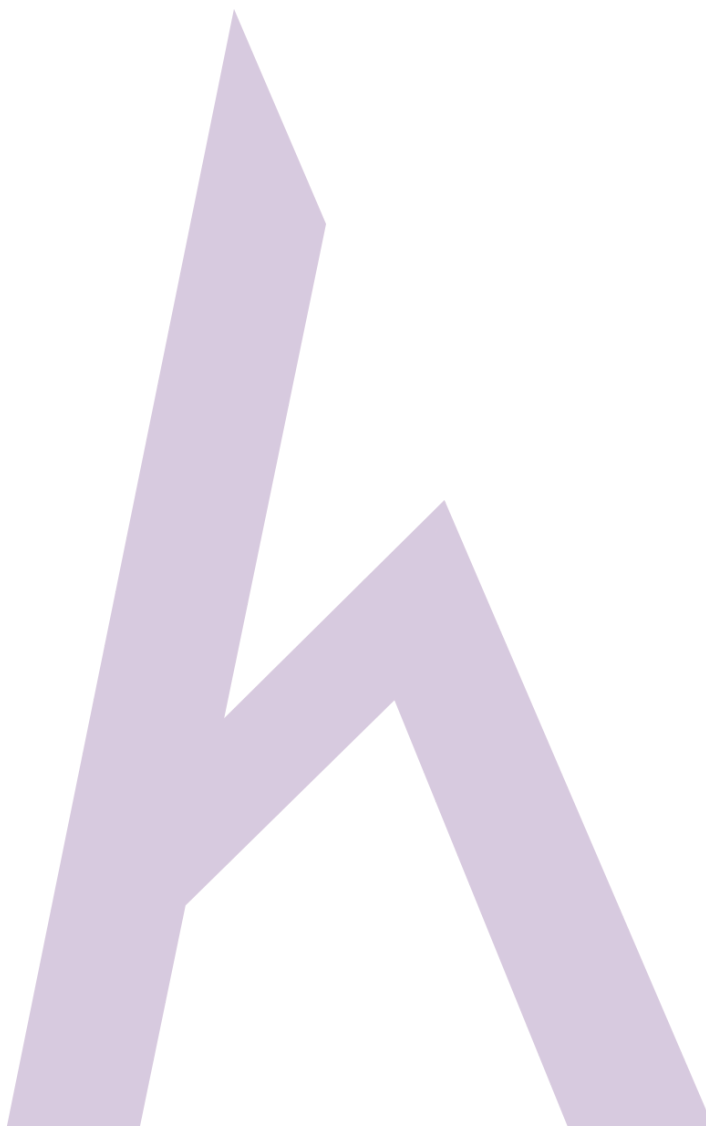
Ví dụ: Người nhận được chuyển hướng đến trang web ngân hàng giả mạo, yêu cầu thông tin nhạy cảm.

Tương tự, liên kết được chuyển hướng có thể tải xuống bất kỳ tập lệnh độc hại nào trên hệ thống của người nhận tìm nạp thông tin.

Lướt sóng (Shoulder Surfing)

Shoulder Surfing là một phương pháp thu thập thông tin bằng cách đứng đằng sau một mục tiêu khi hắn ta đang tương tác với thông tin nhạy cảm. Bằng cách lướt sóng này, mật khẩu, số tài khoản hoặc thông tin bí mật khác có thể được thu thập tùy thuộc vào sự bất cẩn của đối tượng.

Dumpster Diving



Dumpster Diving là quá trình tìm kiếm kho báu trong thùng rác. Kỹ thuật này cũ hơn nhưng vẫn hiệu quả.

Nó bao gồm truy cập vào thùng rác của mục tiêu như thùng rác máy in, bàn người dùng, thùng rác của công ty để tìm hóa đơn điện thoại, thông tin liên hệ, thông tin tài chính, mã nguồn và tài liệu hữu ích khác.

Công cụ Footprinting (Footprinting Tool)

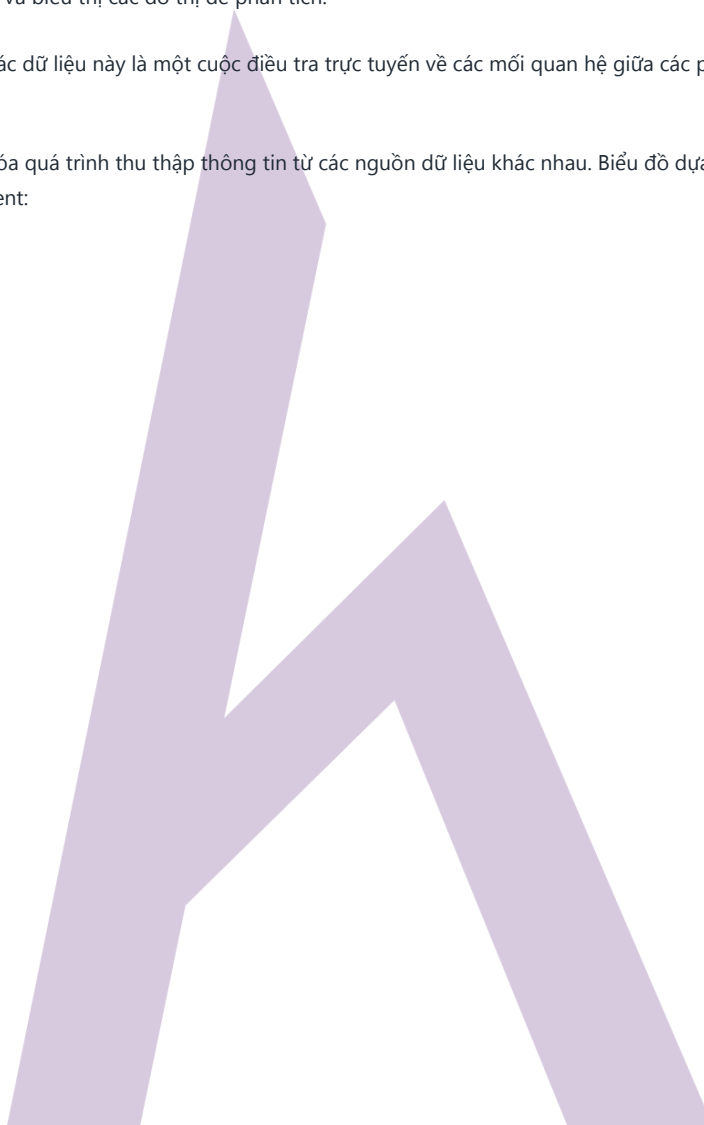
Maltego

Maltego là một công cụ **khai thác dữ liệu** được cung cấp bởi Paterva.

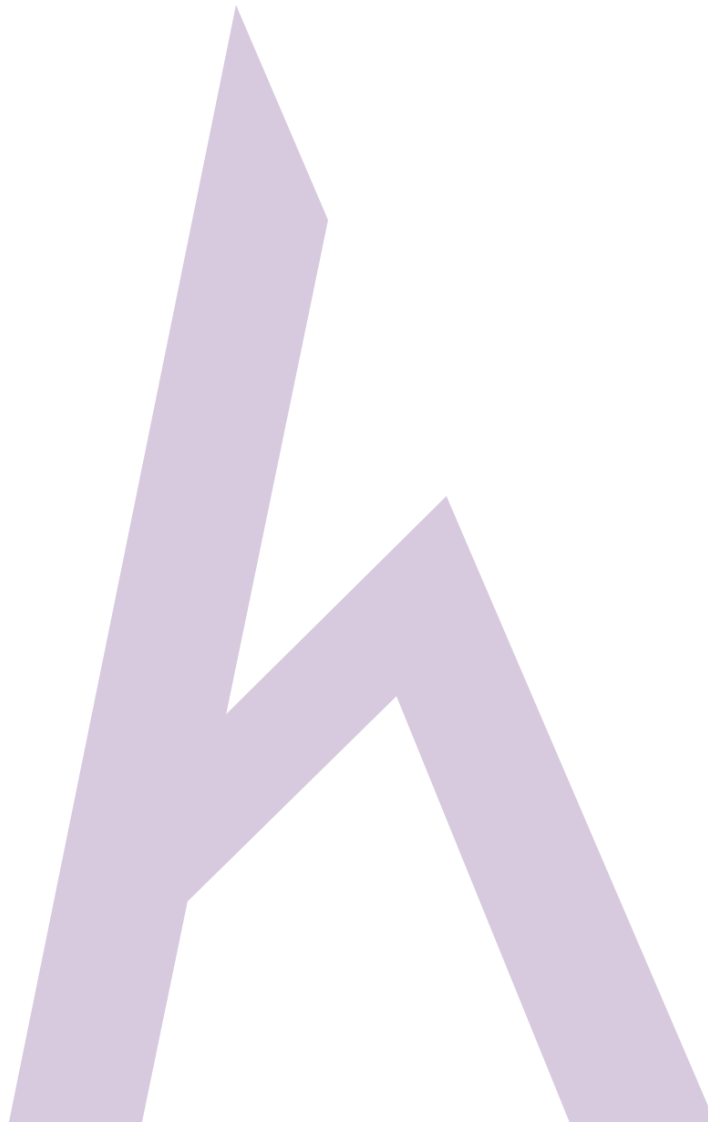
Công cụ tương tác này thu thập dữ liệu và biểu thị các đồ thị để phân tích.

Mục đích đo lường của công cụ khai thác dữ liệu này là một cuộc điều tra trực tuyến về các mối quan hệ giữa các phần thông tin thu được từ nhiều nguồn khác nhau nằm trên internet.

Sử dụng Transform, Maltego tự động hóa quá trình thu thập thông tin từ các nguồn dữ liệu khác nhau. Biểu đồ dựa trên nút biểu thị thông tin này. Có 3 phiên bản phần mềm Maltego Client:



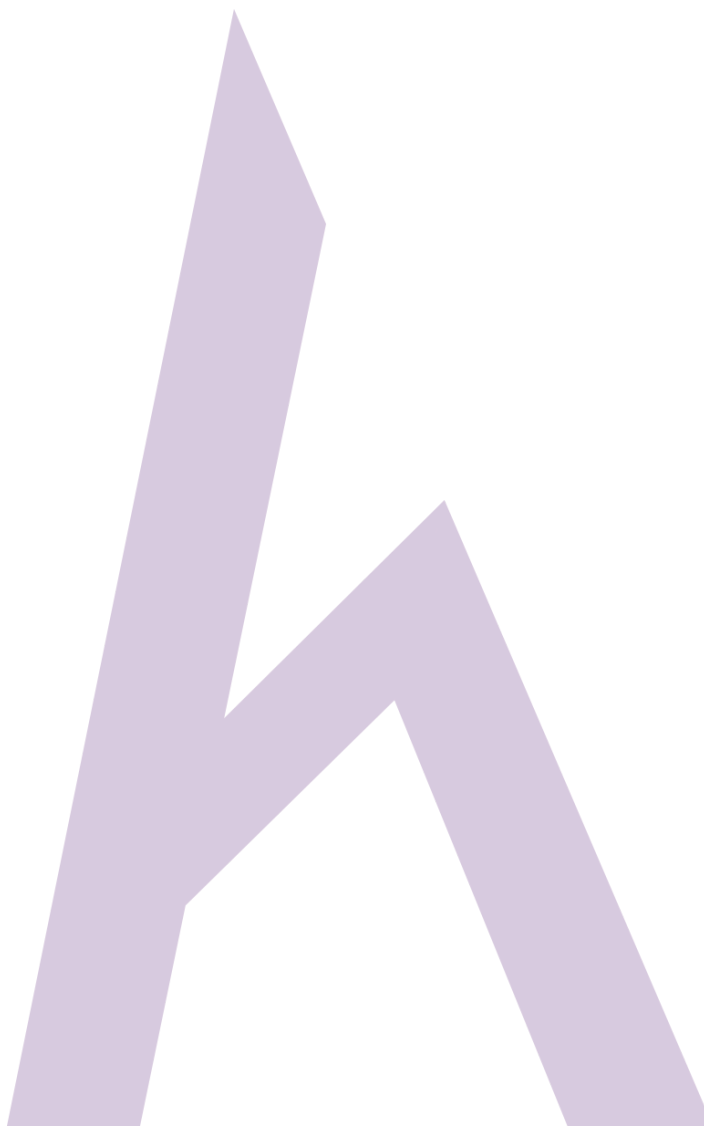
- Maltego CE
- Maltego Classic
- Maltego XL

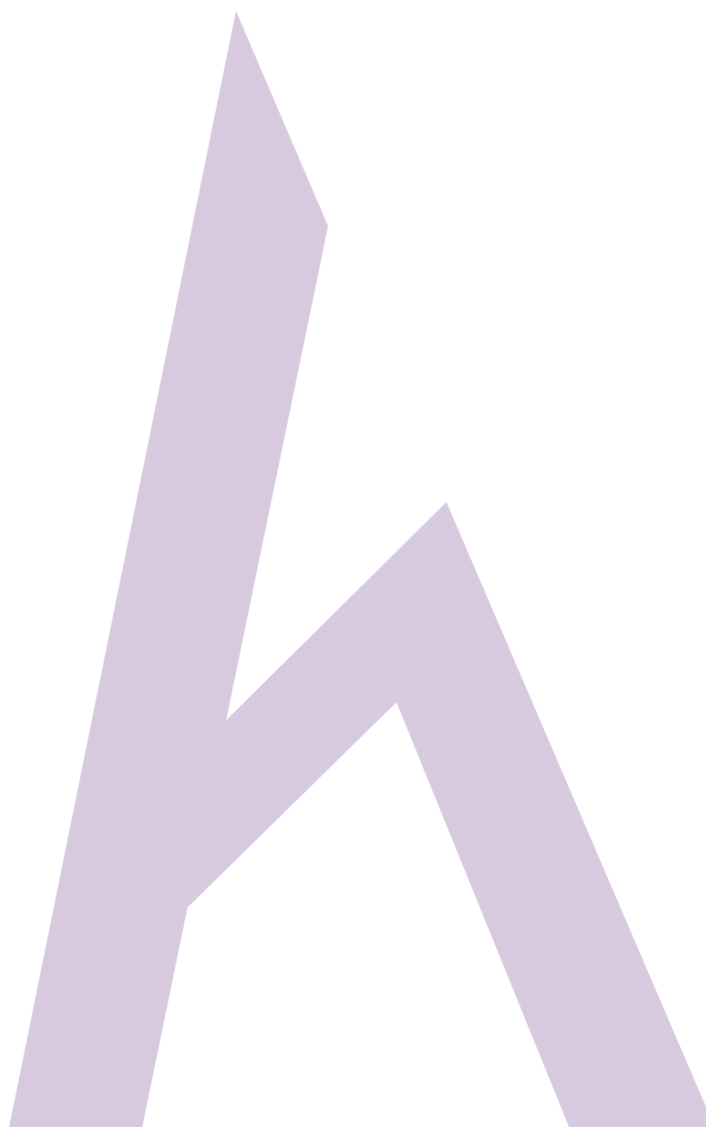


Lab 02-1: Tổng quan về công cụ Maltego (Maltego Tool Overview)

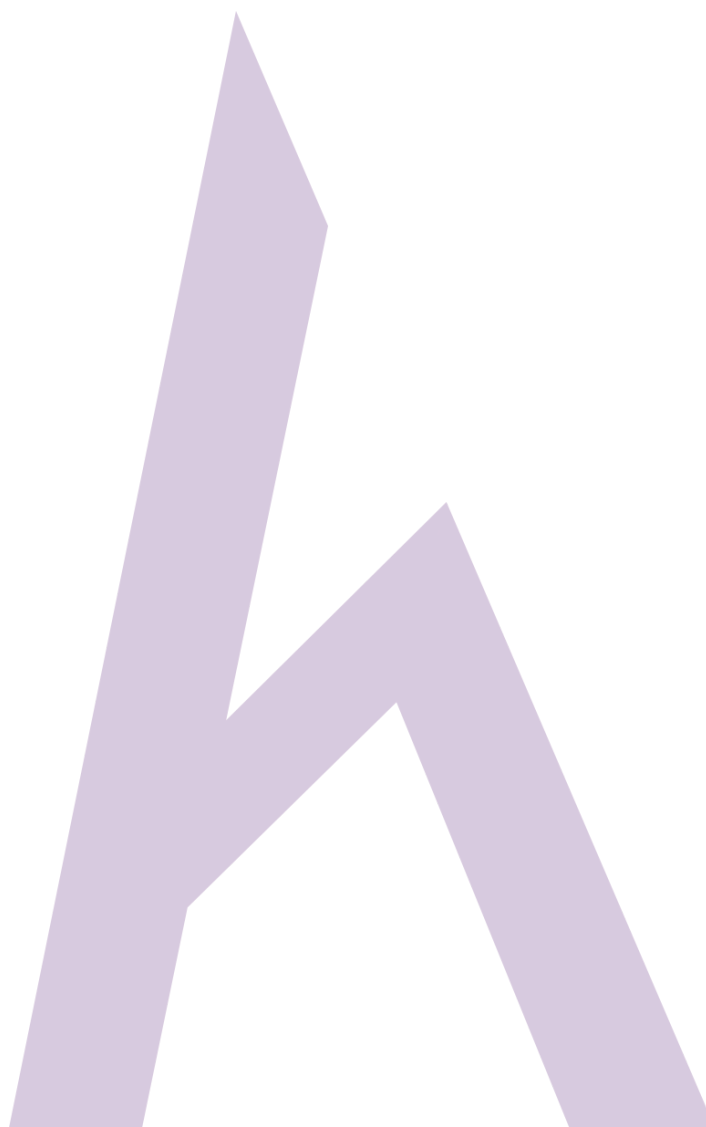
Cách thức:

Bạn có thể tải xuống Maltego từ trang web **Paterva** (ví dụ: <https://www.paterva.com>). Yêu cầu đăng ký để tải xuống phần mềm. Sau khi tải xuống, cài đặt cần có khóa cấp phép để chạy ứng dụng có đầy đủ các tính năng.

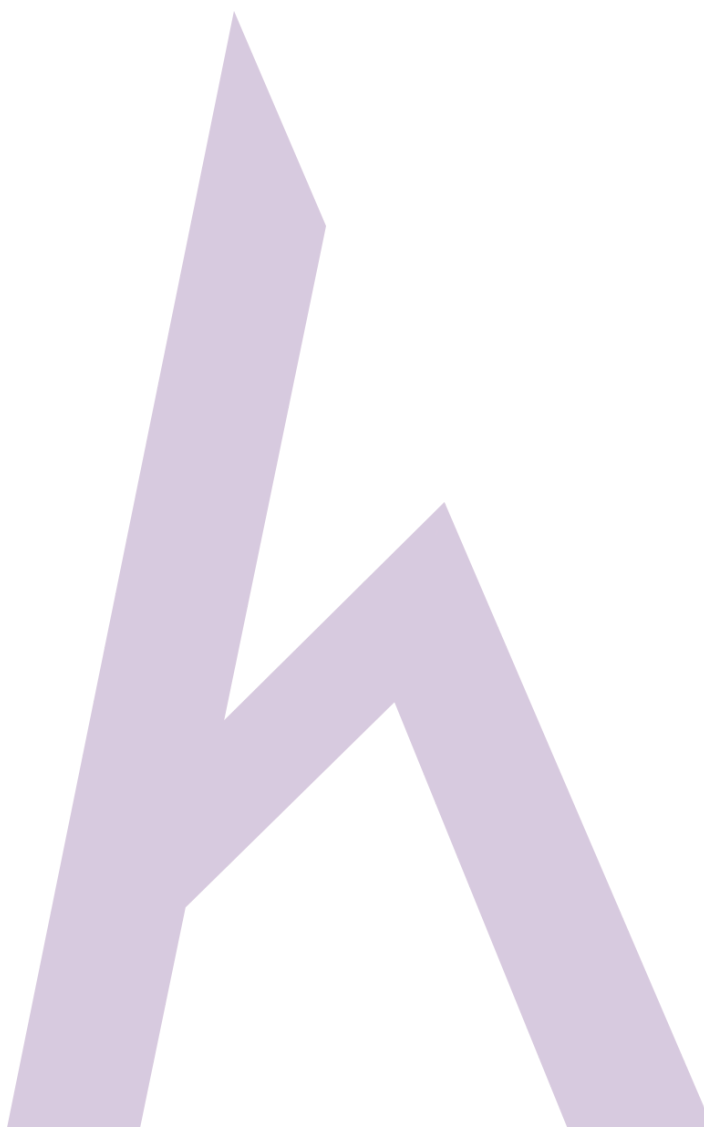


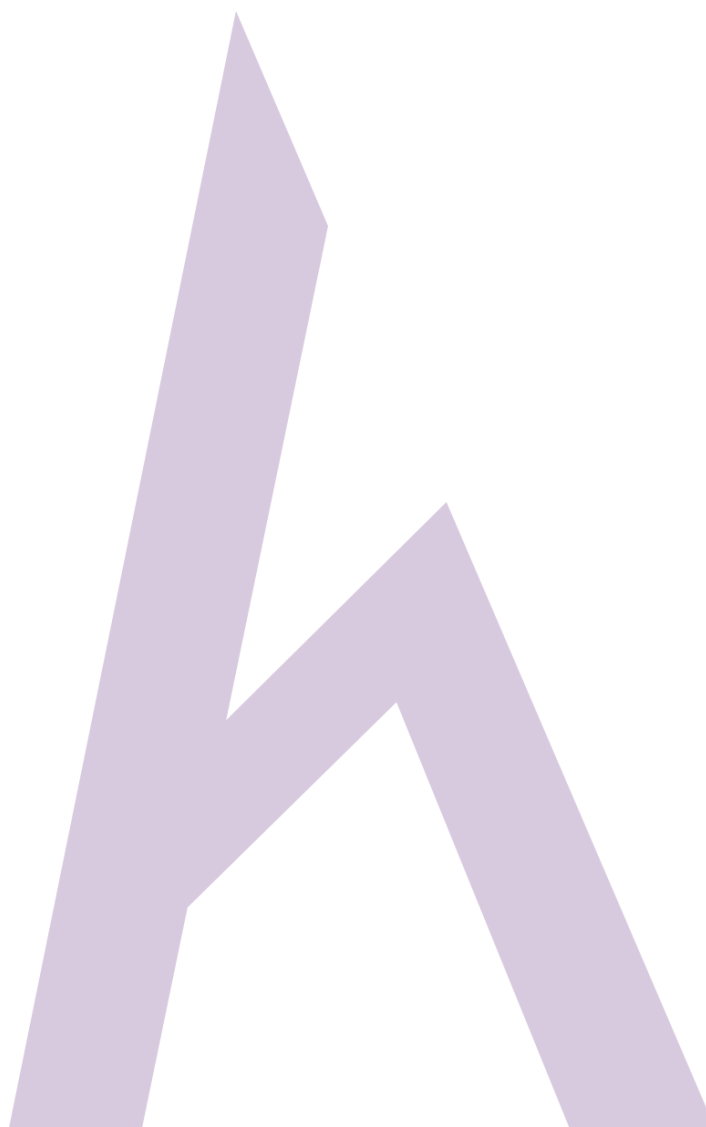


Trên đây là trang chủ của **Maltego Community Edition** (CE). Trên cùng, nhấp vào  tạo biểu đồ đồ thị mới



Bạn có thể chọn bằng **Entity** theo loại truy vấn của bạn. Trong trường hợp của chúng tôi, Ví dụ, Tên miền được chọn.





Chỉnh sửa tên miền và nhấp chuột phải vào biểu tượng tên miền để chọn Run Transform Option. Chọn tùy chọn và quan sát kết quả được hiển thị.

Các tùy chọn có sẵn là:

- Tất cả chuyển đổi (All Transform)
- DNS từ tên miền (DNS from Domain)
- Chi tiết chủ sở hữu tên miền (Domain Owner details)
- Địa chỉ email từ miền (Email addresses from Domain)
- Tập và dữ liệu từ miền (Files and Documents from Domain)

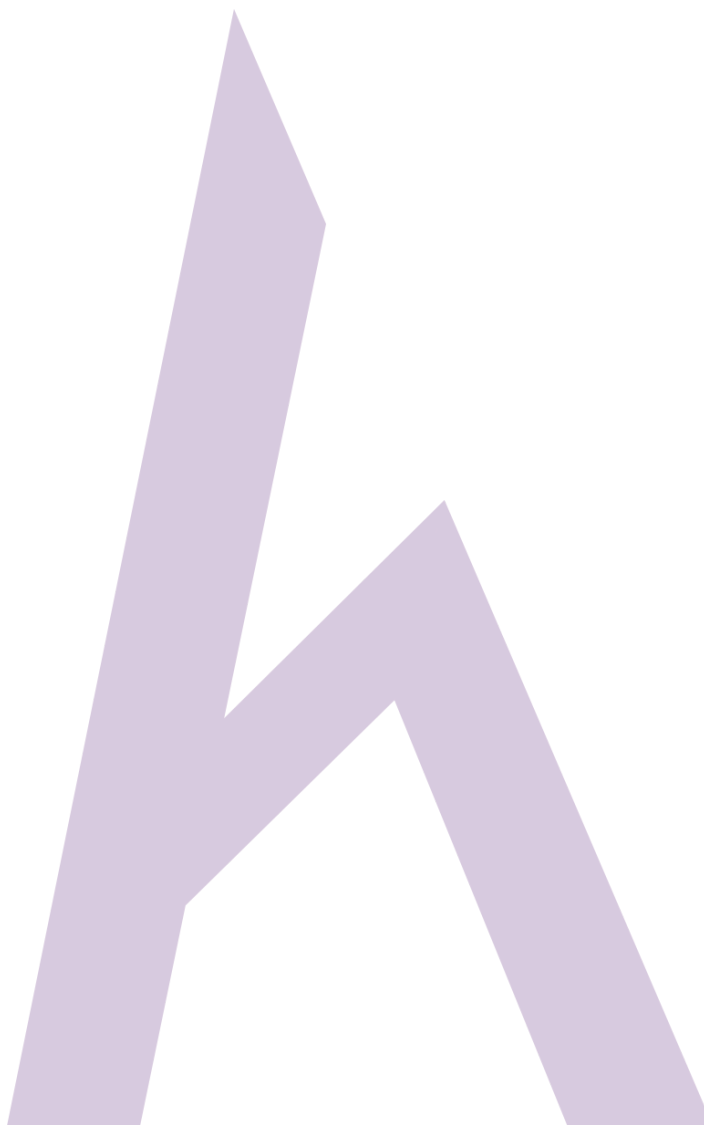
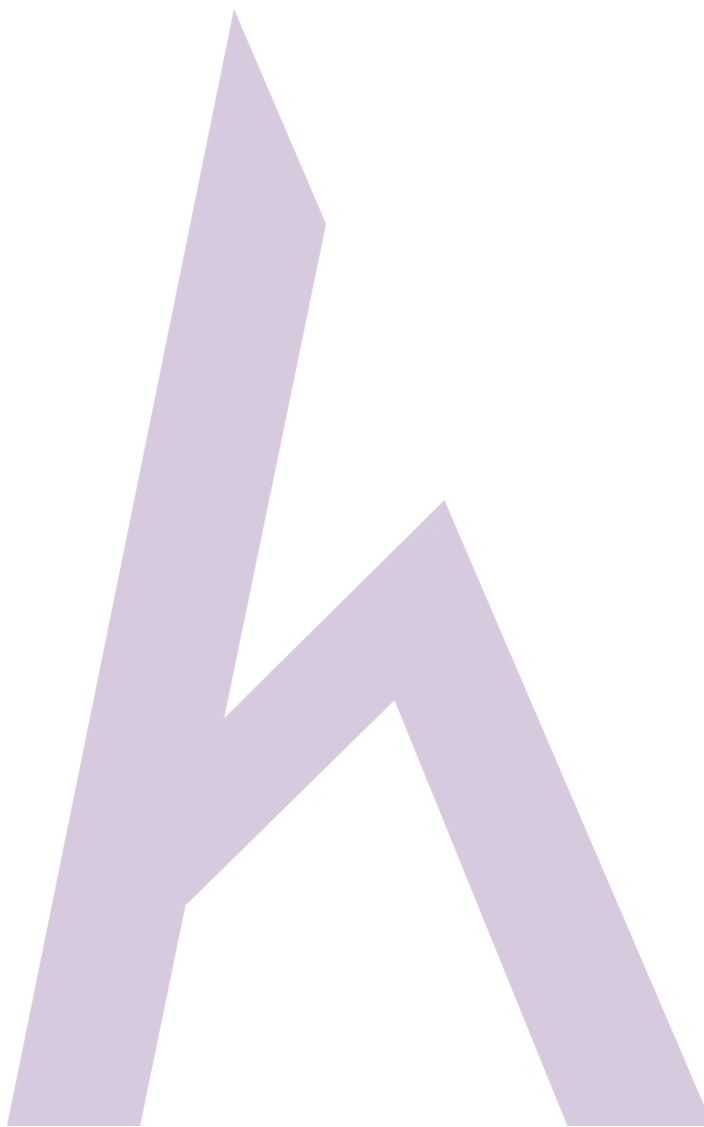
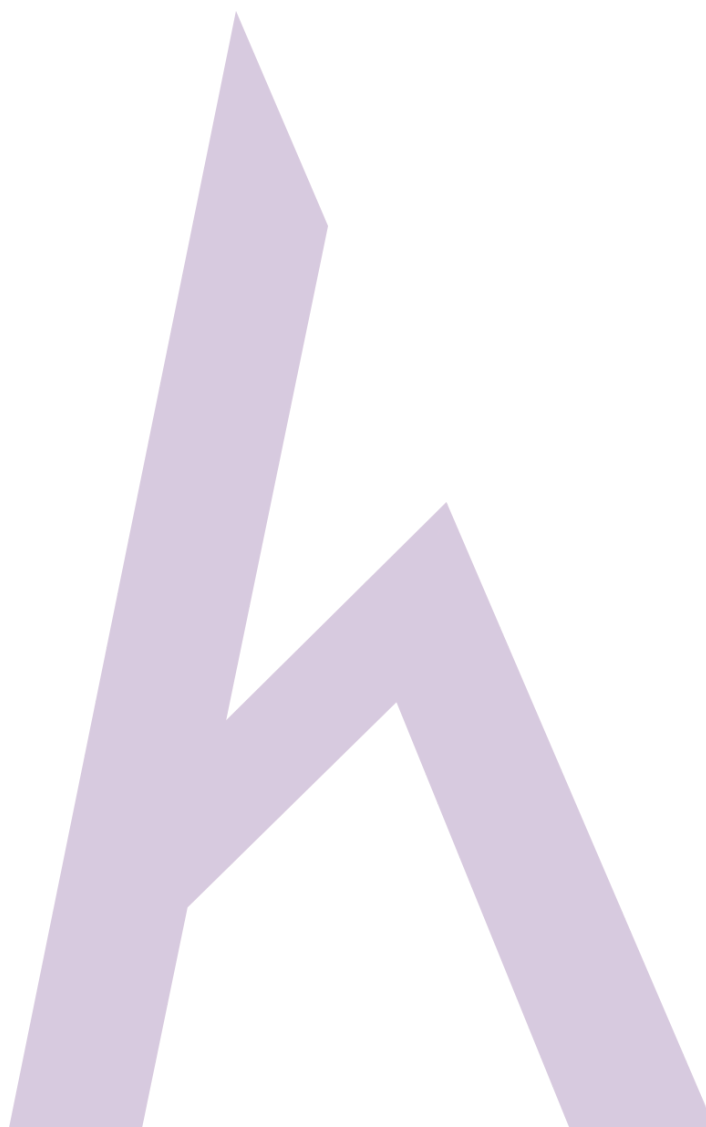


Figure 2-47 Maltego



Recon-ng

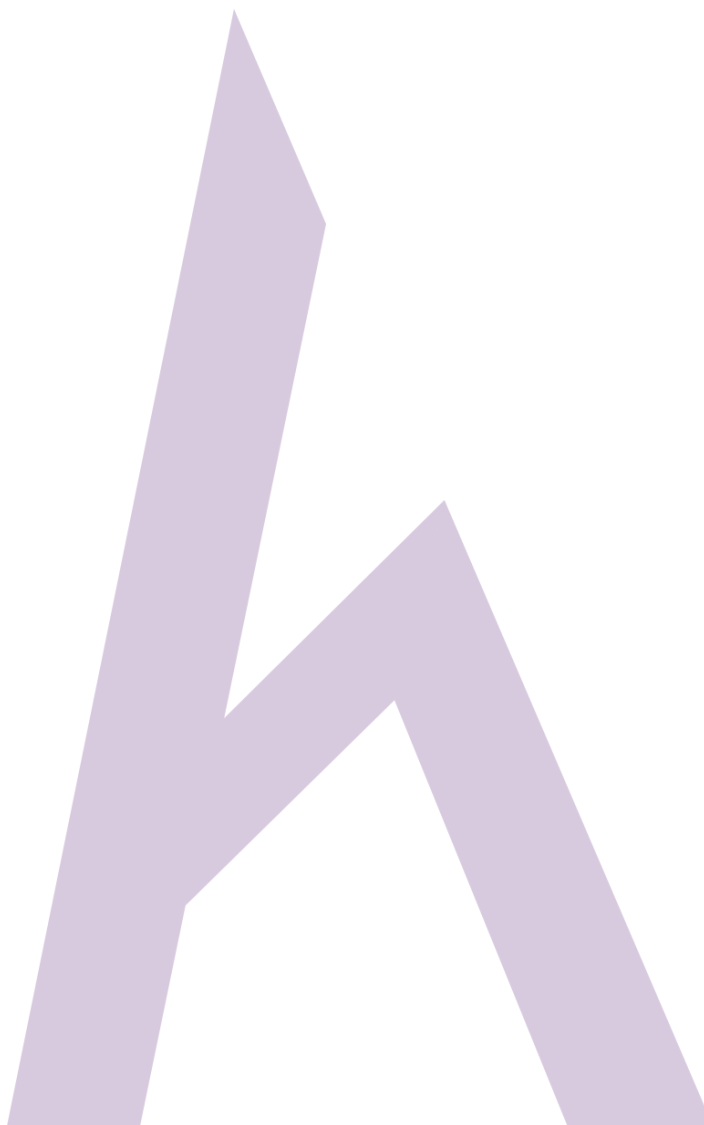


Recong0-ng là một công cụ thăm dò được dùng cho mục đích thu thập thông tin cũng như phát hiện các mạng máy tính. Công cụ này được viết bằng ngôn ngữ Python, có các Mô-đun độc lập, có thể tương tác với cơ sở dữ liệu và một số tính năng khác nữa. Bạn có thể tải về công cụ này từ www.bitbucket.org. **Recong0-ng** yêu cầu sử dụng hệ điều hành Linux

Lab 02-2: Tổng quan về Recon-ng (Recon-ng Overview)

Cách thức:

Mở **Kali Linux** và chạy **Recon-ng**



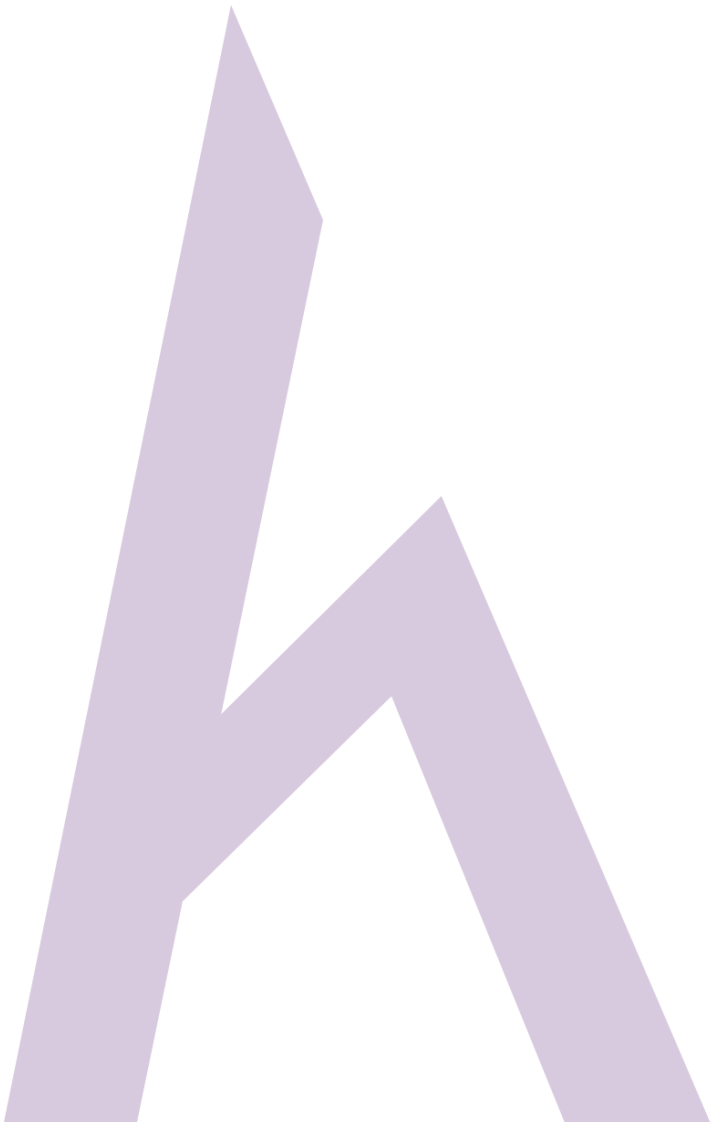
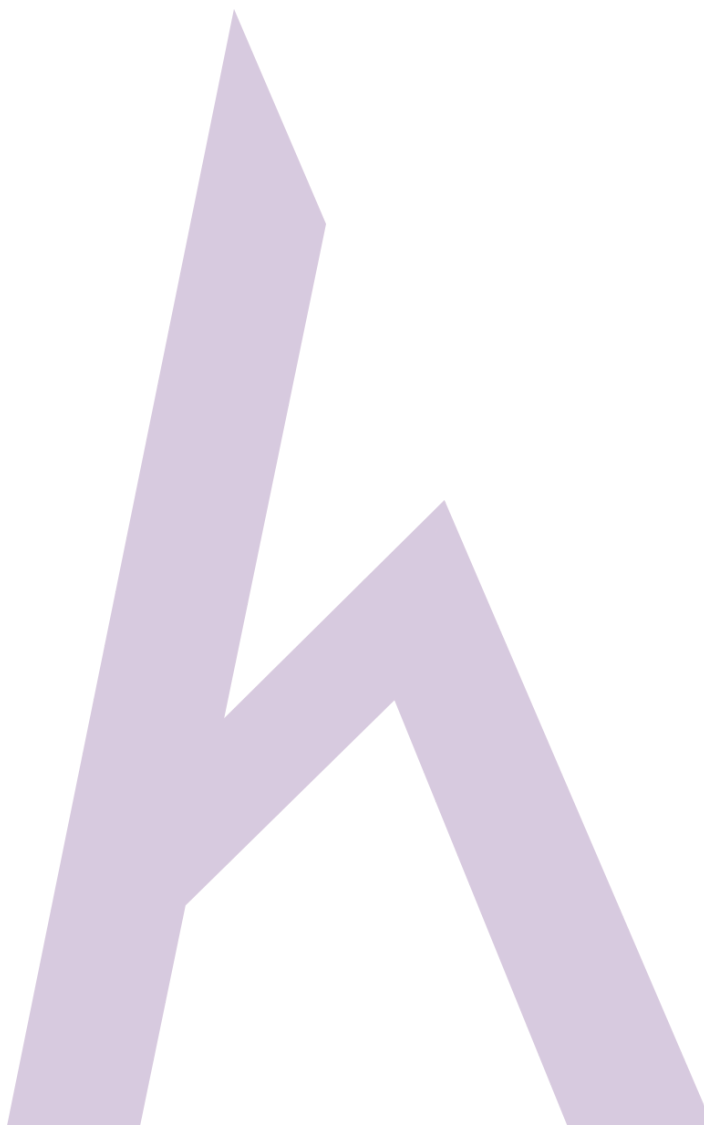


Figure 2-48 Recon-ng

Chạy ứng dụng **Recon-ng** hoặc mở **terminal** của **Kali-Linux** và gõ **recon-ng** và nhấn **enter**.

Figure 2-49 Recon-ng (Show module command)

Nhập lệnh "**show modules**" để hiển thị tất cả các module độc lập có sẵn.



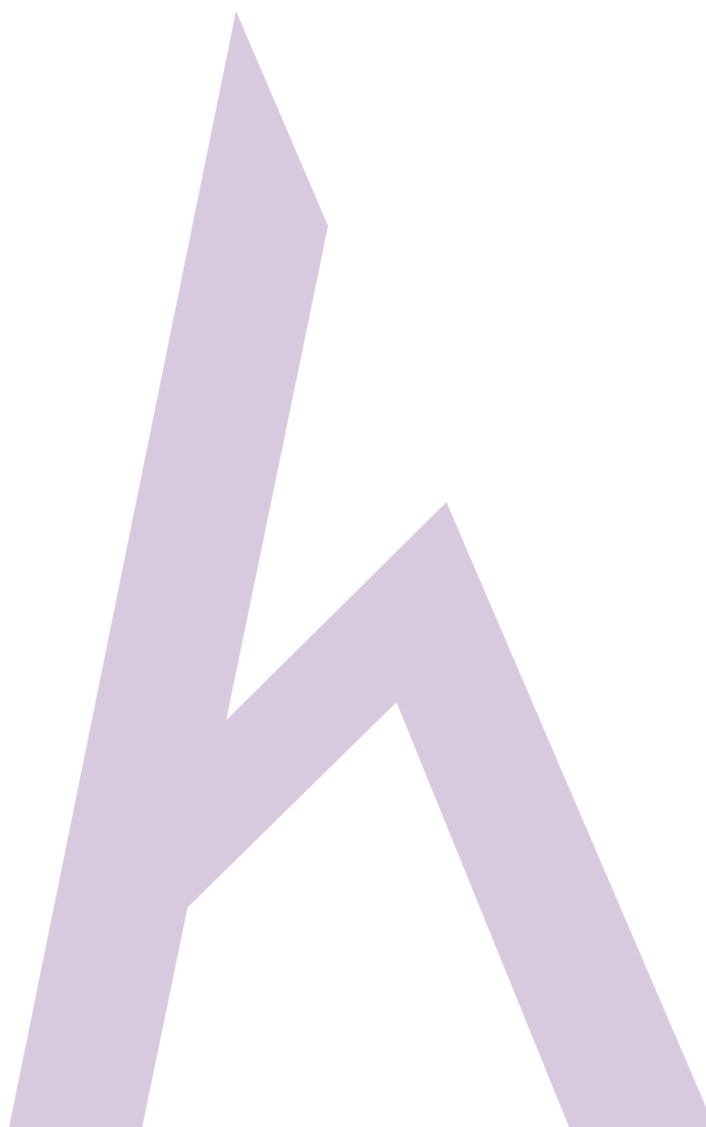
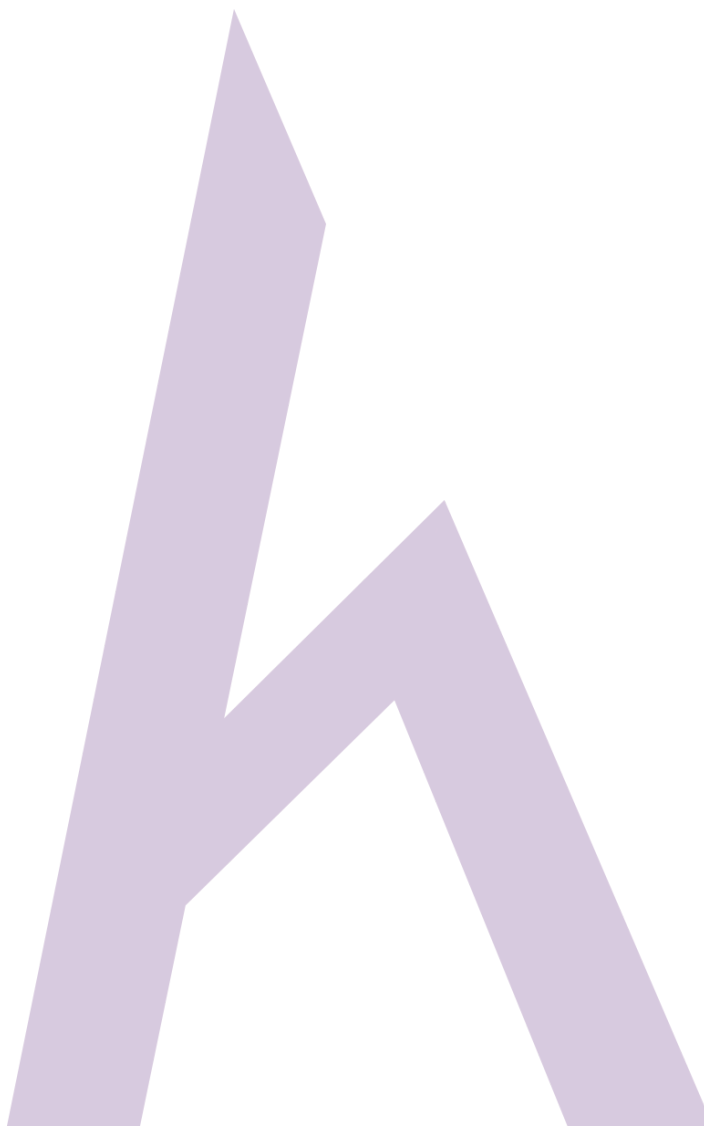


Figure 2-50 Recon-ng (Search command)

Bạn có thể tìm kiếm bất kỳ **Entity** (đối tượng) nào trong module. Ví dụ, trong hình trên, lệnh “**Search Netcraft**” được sử dụng.



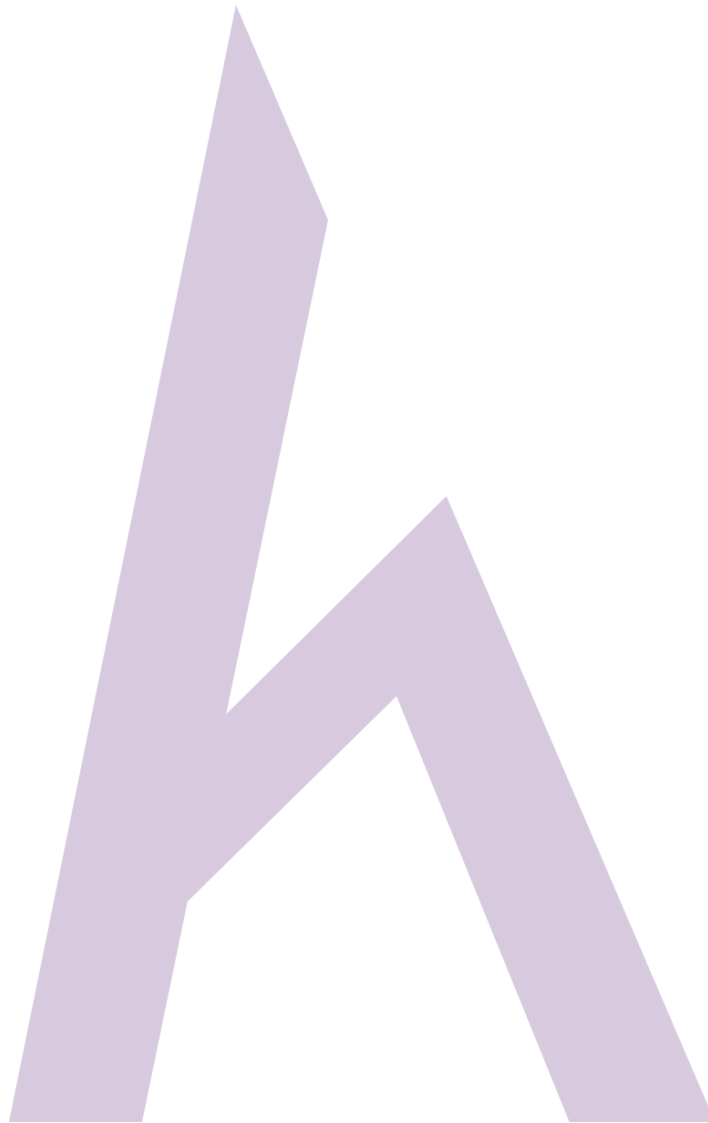
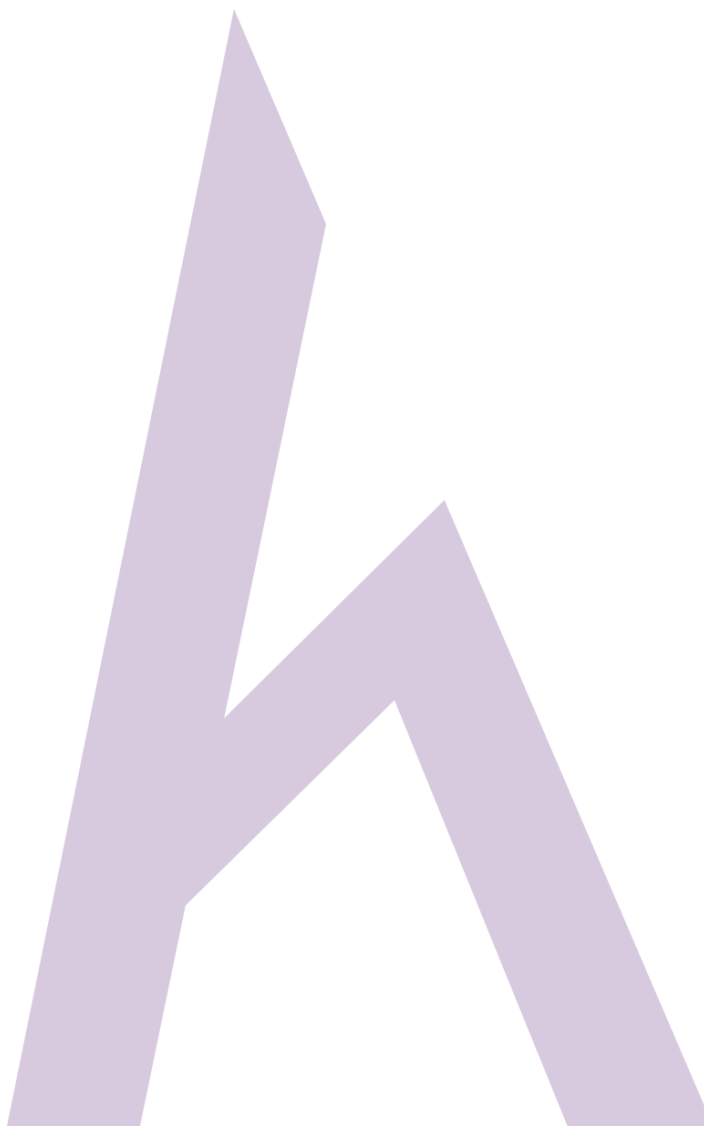


Figure 2-51 Using Netcraft through Recon-ng

Để sử dụng module Netcraft, hãy sử dụng cú pháp lệnh **"use recon/domain-hosts/Netcraft"** và nhấn **enter**.



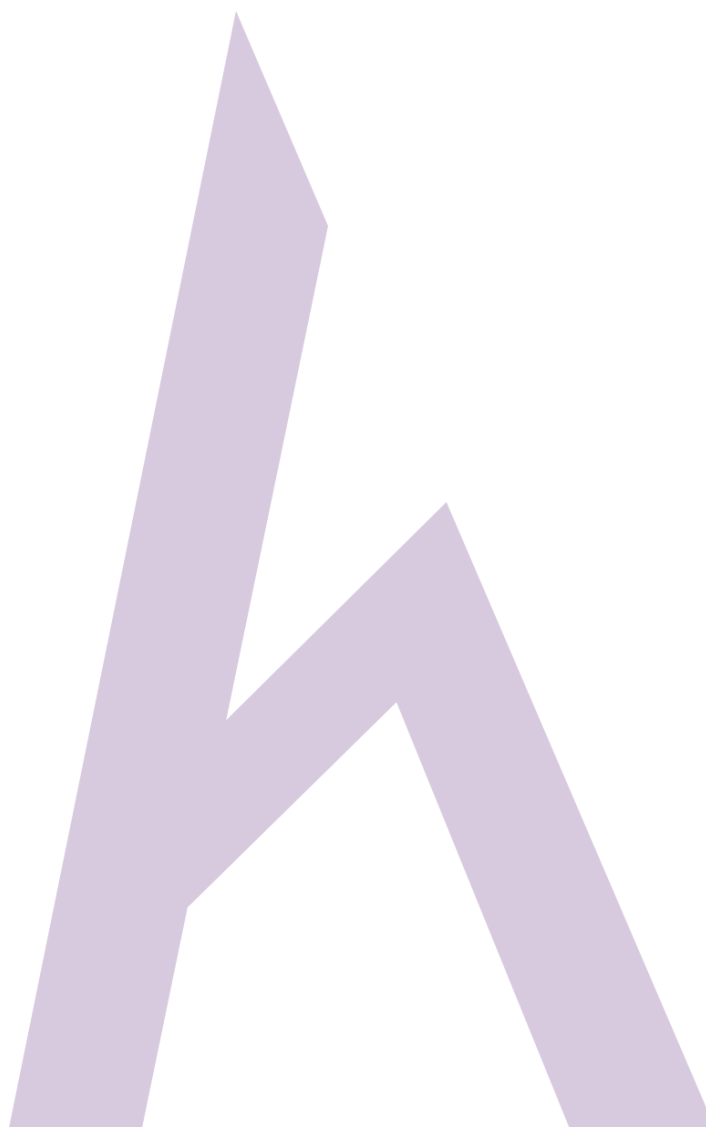


Figure 2-52 Searching for Target Domain

Đặt nguồn bằng lệnh "**set source [domain]**." Nhấn **enter** để tiếp tục. Nhập **Run** thực hiện và nhấn **Enter**.

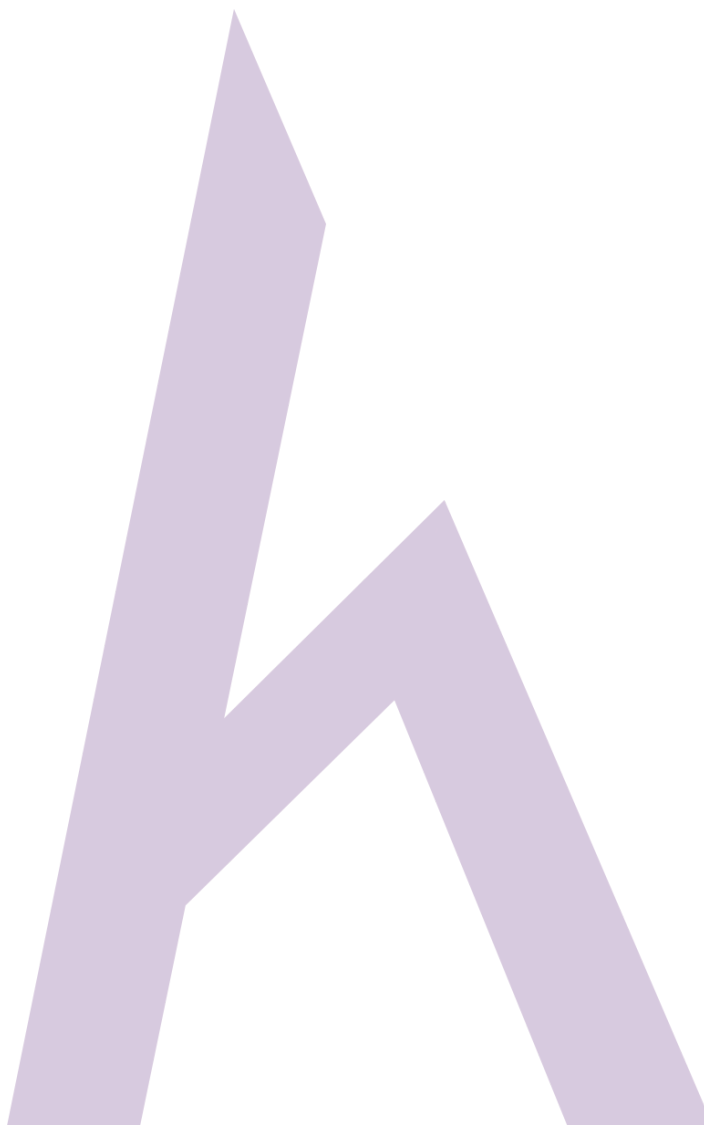
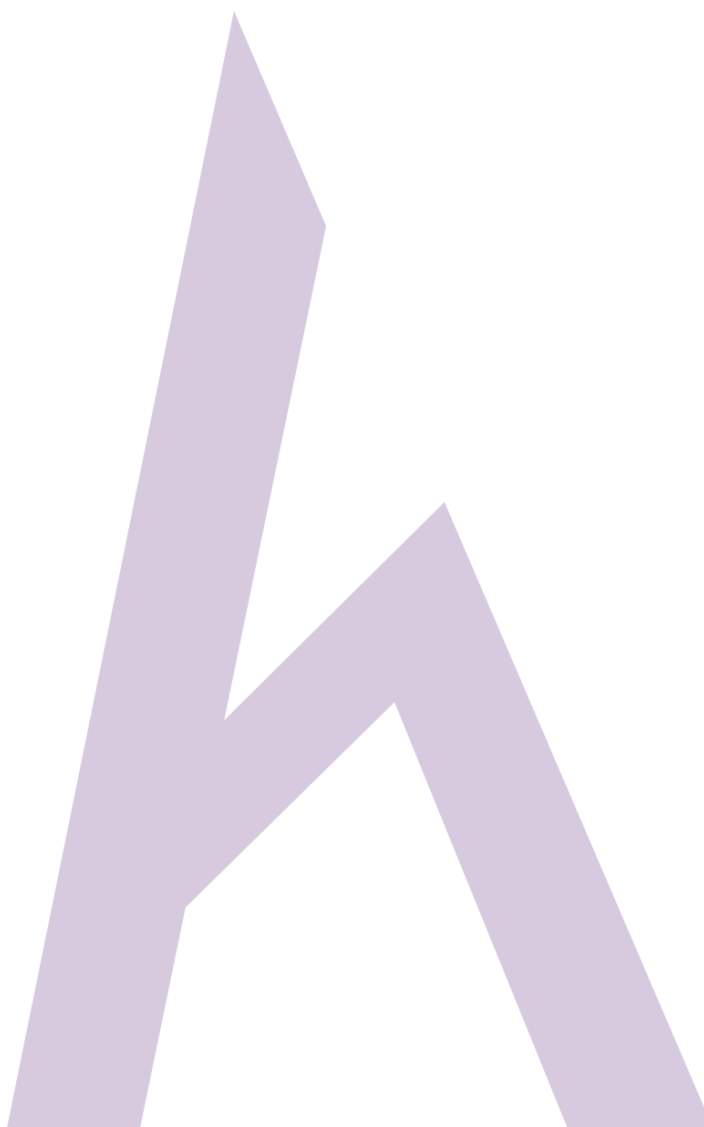


Figure 2-53 Search Result of Target Domain



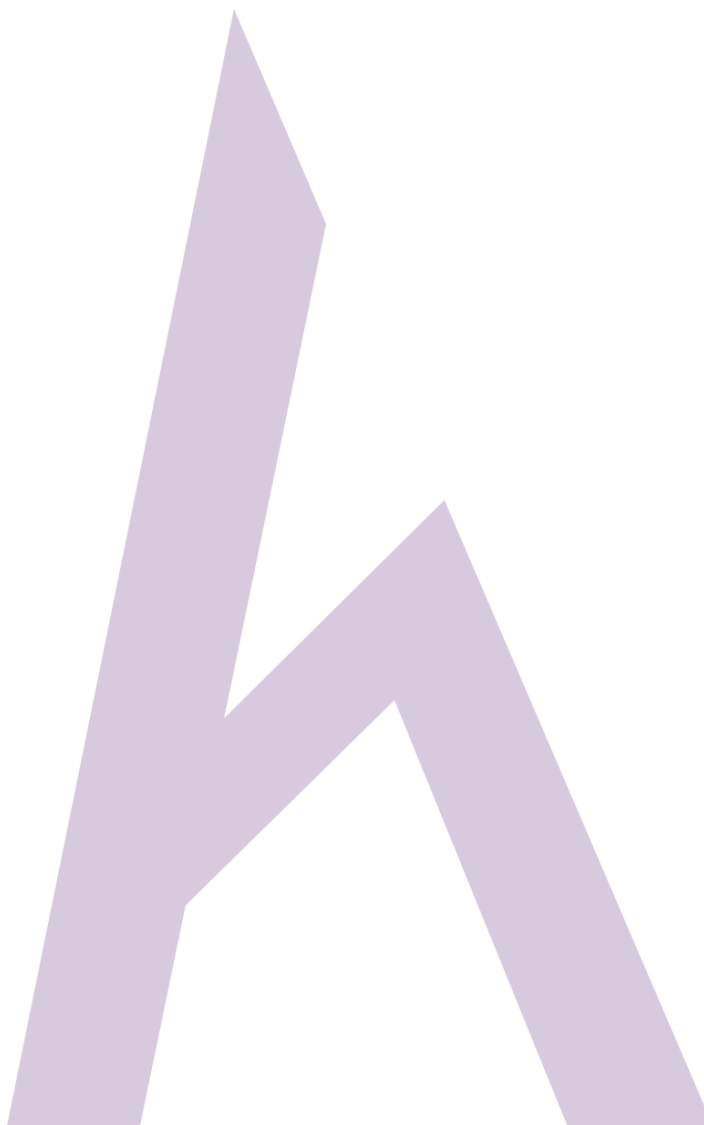
Recon-ng đang thu thập thông tin của miền mục tiêu.

Công cụ Footprinting bổ sung (Additional Footprinting Tools)

FOCA là viết tắt của **Fingerprinting Organizations with Collected Archives**.

Công cụ FOCA tìm siêu dữ liệu và thông tin ẩn khác trong tài liệu có thể tìm thấy trên các trang web.

Các tìm kiếm được quét có thể được tải xuống và phân tích. FOCA là một công cụ tác động mạnh có thể hỗ trợ nhiều loại tài liệu bao gồm Open Office, Microsoft Office, Adobe InDesign, PDF, SVG và các loại tài liệu khác. Tìm kiếm sử dụng ba công cụ tìm kiếm như Google, Bing và DuckDuckGo.



Lab 02-3: Tổng quan về công cụ FOCA (FOCA Tool Overview)

Cách thức:

Download phần mềm FOCA từ <https://www.elevenpaths.com>. Bây giờ, hãy chọn **Project > New Project**.

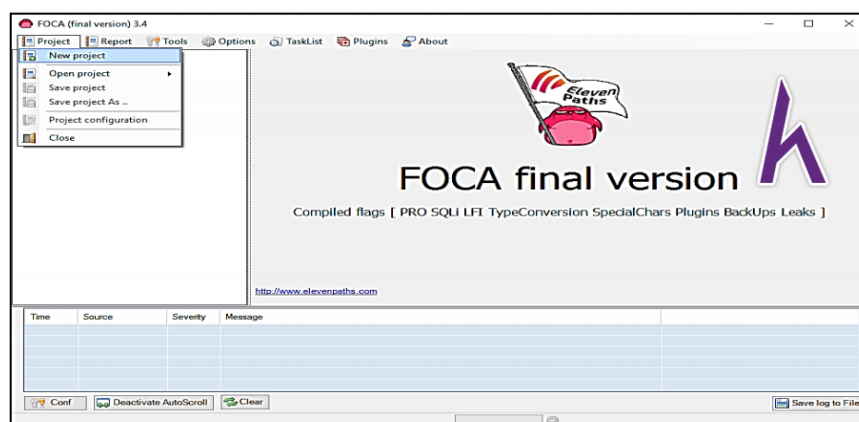


Figure 2-55 Creating New Project using FOCA

Tiếp theo, hãy nhập **tên dự án** (Project name), **tên miền trang web** (Domain website), **Trang web thay thế** (Alternate website) nếu cần thiết, **Thư mục để lưu kết quả** (Directory to save the results), **ngày dự án** (Project date) Nhấn nút **Create** để tiếp tục

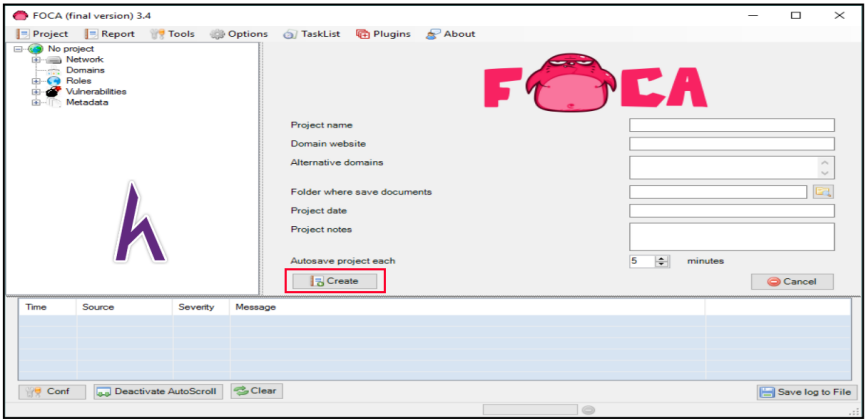
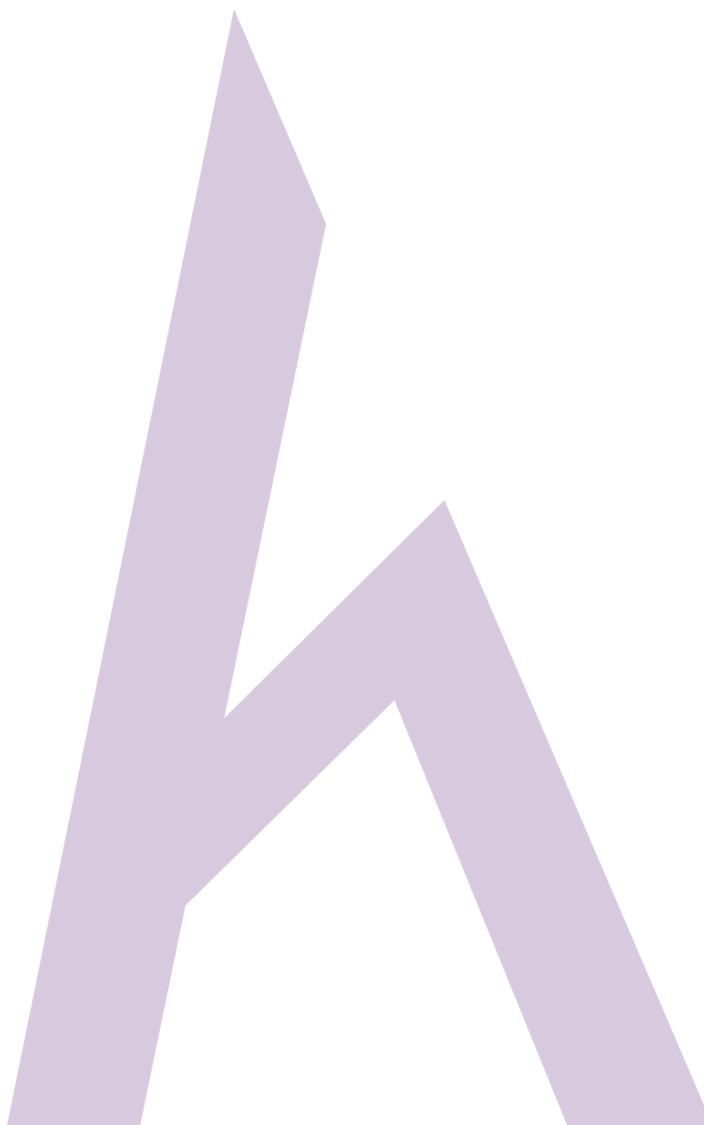


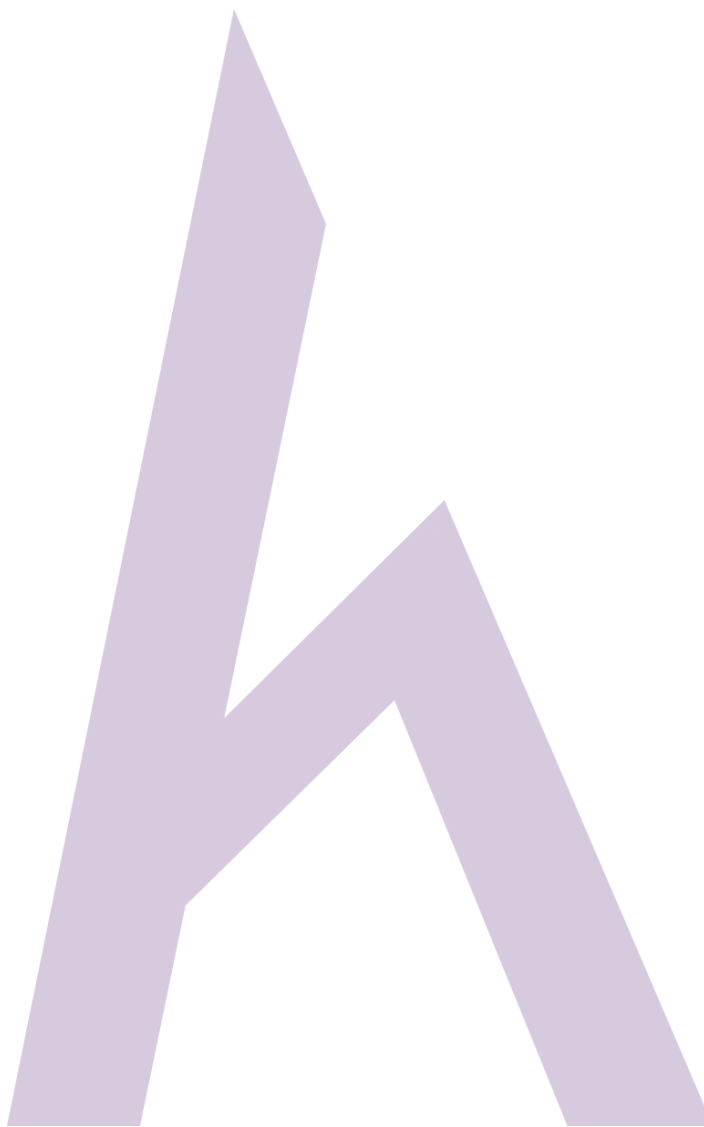
Figure 2-56 Creating New Project using FOCA

Chọn **Search Engines** (công cụ tìm kiếm), **Extensions** (tiện ích mở rộng), và các thông số khác theo yêu cầu, nhấp vào **Search All**

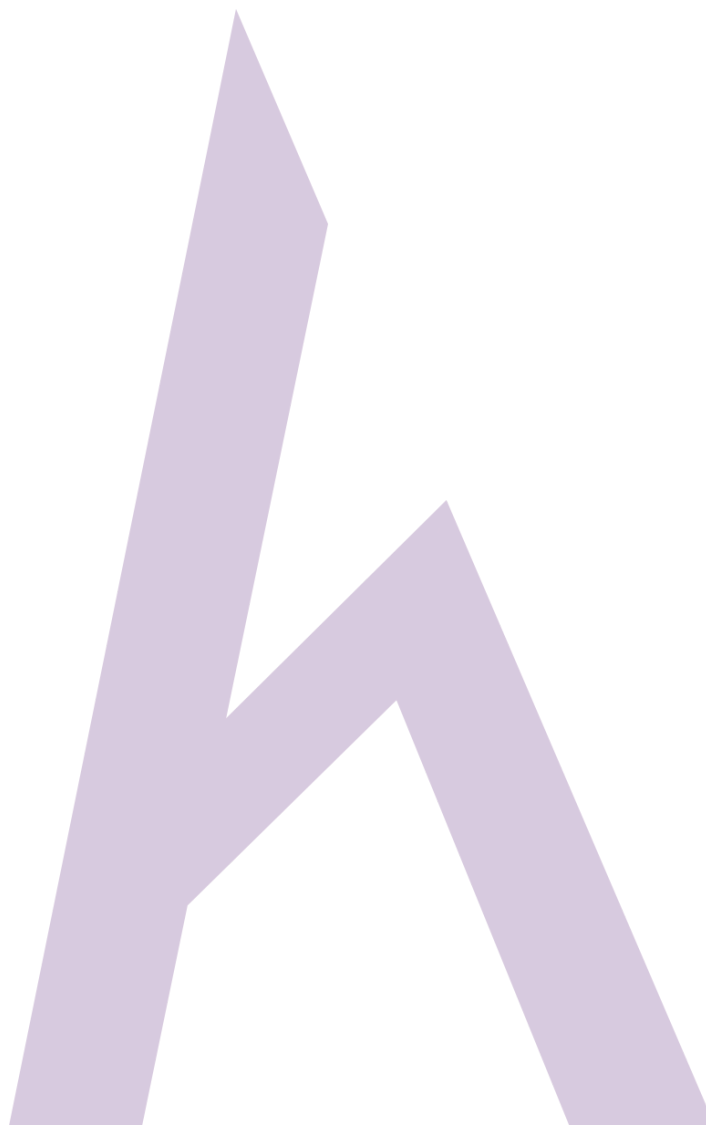
Khi Tìm kiếm hoàn tất, hộp tìm kiếm hiển thị nhiều tệp. Bạn có thể chọn tệp, tải xuống, Trích xuất siêu dữ liệu và thu thập thông tin khác như tên người dùng, ngày tạo tệp và sửa đổi.



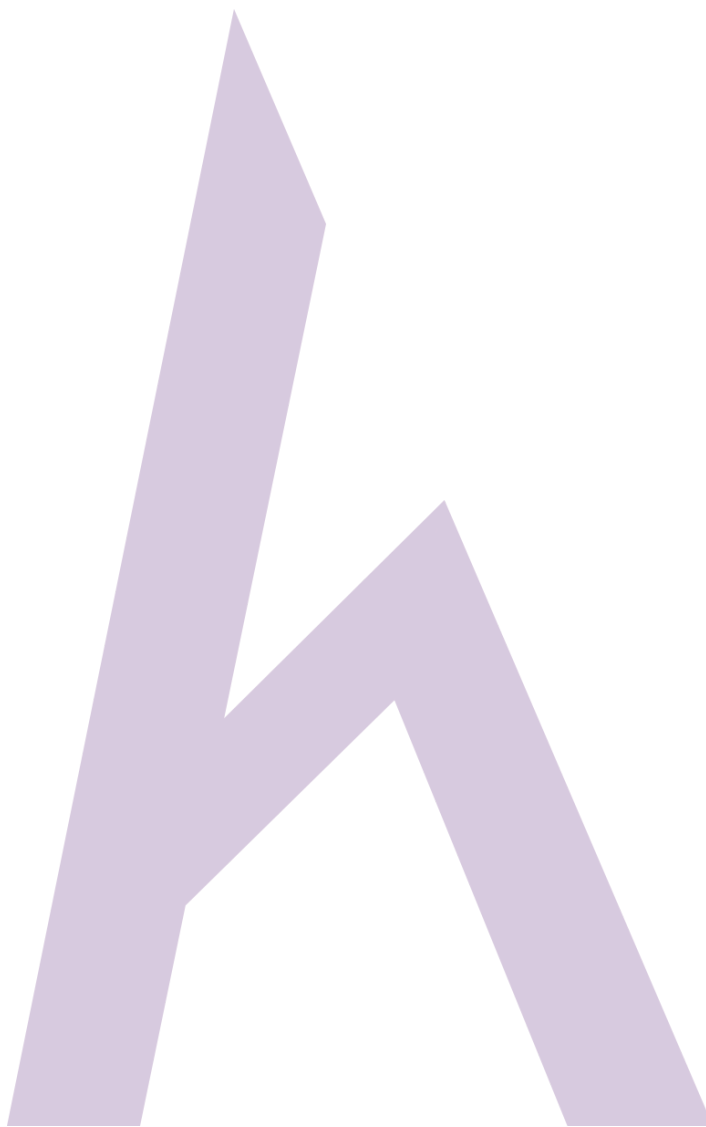
Công cụ dò tìm dấu vết bổ sung



Công cụ	Websites
Prefix Whois	http://pwhois.org
Netmask	http://www.phenoelit.org
DNS-Digger	http://www.dnsdigger.com
Email Tracking Tool	http://www.filley.com
Ping-Probe	http://www.ping-probe.com
Google Hacks	http://code.google.com

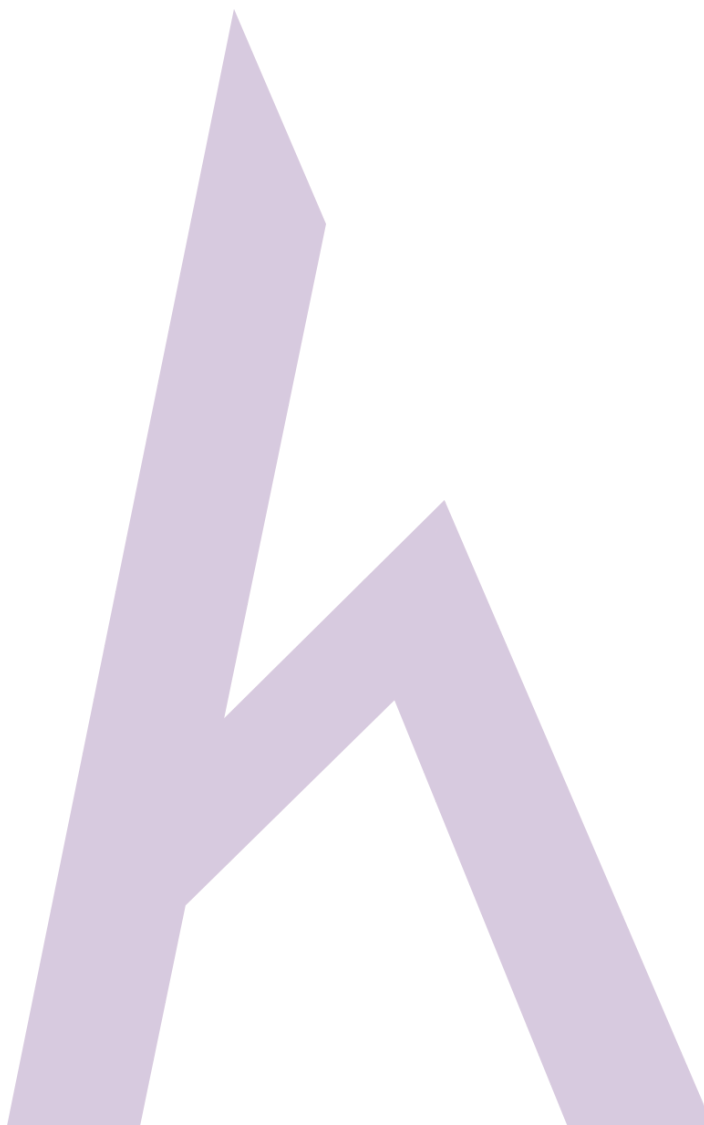


Các biện pháp đối phó của Footprinting



Biện pháp đối phó bao gồm các biện pháp sau để giảm thiểu dấu vết:

- Nhân viên trong một tổ chức phải bị hạn chế truy cập các trang mạng xã hội từ mạng công ty.
- Thiết bị và máy chủ được cấu hình để tránh rò rỉ dữ liệu
- Cung cấp giáo dục, đào tạo và nhận thức về dấu chân, tác động, phương pháp, và biện pháp đối phó với nhân viên của một tổ chức
- Tránh tiết lộ thông tin nhạy cảm trong các báo cáo
- Hàng năm, thông cáo báo chí, v.v
- Ngăn công cụ tìm kiếm lưu vào bộ nhớ cache các trang web.



Mind Map

