How to Use AI to Build an OSINT Search Plan Before You Start Investigating

Maria Cattini | 15/06/2026 | OSINT

Most OSINT mistakes do not begin with the wrong tool.

They begin before the tool is opened.

A researcher starts with a vague question, runs a few searches, saves random links, follows an interesting account, opens a map, checks a screenshot, asks an AI tool for suggestions, and suddenly the investigation has no shape. There are many fragments, but no plan.

The problem is not lack of effort.

The problem is that the search started before the question was operational.

AI can help at this stage. Not by finding the truth for you. Not by replacing search engines, archives, maps, registries, or primary sources. Its useful role is more basic: it can help you turn a vague investigative question into a structured search plan.

That plan should tell you what to look for, where to look, which words to test, which languages may matter, what evidence would count, and what risks could mislead you.

Before you investigate, build the search plan.

Start With the Real Question

Many investigations begin with a sentence that is too broad to search well.

Examples:

- Who is behind this website?
- Is this video real?
- Is this company connected to another company?
- Did this account post the original image?
- Is this claim about a protest accurate?
- Are these profiles controlled by the same person or organization?

These are reasonable questions, but they are not yet search plans.

The first step is to make the question more precise.

Instead of:

Who is behind this website?

write:

What public traces can connect this website to a person, organization, infrastructure, domain owner, social profile, company, or previous project?

Instead of:

Is this video real?

write:

Can the location, date, event, and original publication context of this video be independently checked?

This shift matters.

A broad question invites random searching. An operational question defines what can be checked.

AI can help you rewrite the question.

Prompt:

Turn this vague OSINT question into a precise investigative question. Separate what can be verified from what may remain uncertain. Question: [paste your question]

Do not accept the output automatically. Edit it until the question is specific enough to guide a search.

Define the Objects of the Search

An OSINT search plan needs objects.

The object is the thing you are trying to examine: a domain, a username, an image, a video, a company, a location, a wallet, a document, a phone number, a public profile, an email address, a post, or a claim.

If you do not define the object, the search will expand too quickly.

Use a simple table:

Object	What It Is	What It May Reveal	Main Risk
Domain	Website address	infrastructure, archive history, related pages	privacy-protected registration
Username	Public handle	cross-platform activity, reused identity signals	false matches
Image	Visual file or screenshot	location, event, earlier versions	edited or cropped context
Company name	Legal or public entity	registries, officers, addresses, related firms	same-name confusion
Social post	Public claim or media	timeline, source, interaction network	deleted or reposted content

AI can help list the possible objects, especially when the case has several moving parts.

Prompt:

Extract the searchable objects from this case description. Group them by type: people, organizations, accounts, domains, media, locations, documents, technical indicators, and claims. For each object, explain what it may help verify and what false positive risk it creates. Case description:

[paste your notes]

The goal is not to create a long list. The goal is to decide where the investigation should begin.

Build Search Paths, Not Just Search Queries

A query is one search.

A search path is a sequence.

For example, if the object is a domain, a search path may look like this:

1. Check the live website.
2. Save the URL and visible claims.
3. Search archived versions.
4. Compare old and current pages.
5. Check public domain and DNS information where available.
6. Search the domain in exact match.
7. Search unique page text.
8. Search connected emails, usernames, social links, or company names.
9. Record what each source supports.

If the object is a video, the path changes:

1. Preserve the original post.
2. Identify the earliest visible upload.
3. Extract visual clues.
4. Check location indicators.
5. Compare with maps, street-level imagery, or satellite imagery.
6. Check date clues such as weather, light, events, clothing, signage, or public reports.
7. Search for earlier versions of the same media.
8. Record what is confirmed, likely, or still unverified.

AI can suggest search paths, but you should adapt them to the case.

Prompt:

Create an OSINT search path for this object. Include the first sources to check, the order of checks, what each step can verify, what it cannot verify, and common false positives. Object: [domain / username / image / video / company / claim] Context: [short case description]

This is where AI becomes useful: it helps you avoid opening ten tabs before knowing why they matter.

Generate Queries in Layers

Good OSINT search is not one query. It is a set of query layers.

Start narrow.

Then expand.

Then translate.

Then search by related objects.

For a company or organization, query layers may include:

• exact name;
• exact name plus country or city;
• name plus director, founder, officer, grant, contract, sanction, lawsuit, procurement, partnership, domain;
• local-language spelling;
• abbreviations;
• former names;
• associated addresses;
• unique phrases from public pages;
• related domains or social handles.

For a social media claim, query layers may include:

• exact quote;
• key phrase without punctuation;
• platform-specific search;
• account handle;
• image or video caption;
• translated terms;
• date-limited searches;
• local media keywords;
• archived versions.

AI is good at generating query variations, especially across languages and spelling patterns.

Prompt:

Generate search query layers for this OSINT question. Include exact-match queries, broad discovery queries, local-language variations, date-based queries, and source-specific queries. Do not assume the claim is true. Question: [paste the question] Known objects: [paste objects] Likely countries/languages: [paste if known]

The last sentence is important: do not assume the claim is true.

Search queries can quietly reproduce the claim. If you search only for wording that confirms it, you may miss evidence that contradicts it.

Choose Source Types Before Collecting Links

An OSINT search plan should say which source types matter.

Otherwise, the investigation becomes a pile of links.

For identity or attribution questions, useful source types may include:

• official profiles;
• archived web pages;
• public company registries;
• domain and infrastructure records;
• public documents;
• conference pages;
• media interviews;
• social profile history;
• usernames reused across platforms.

For location questions:

• maps;
• street-level imagery;
• satellite imagery;
• public transport data;
• business listings;
• local news;
• weather records;
• public webcams, when legal and available;
• official event notices.

For timeline questions:

• original upload timestamp;
• archive timestamp;
• edited post history when visible;
• media reports;
• event calendars;
• weather and daylight clues;
• publication sequence across platforms.

AI can help build a source map.

Prompt:

Create a source map for this OSINT question. For each source type, explain what it can verify, what it cannot verify, and how reliable it may be. Question: [paste the question]

This prevents a common mistake: treating every link as equal.

A company registry, a reposted screenshot, a local article, a social media comment, and an archived page do not have the same evidentiary value. They may all be useful, but they support different parts of the analysis.

Add a False Positive Section

Every search plan should include a false positive section.

This is where AI can be especially useful because it can challenge your assumptions before you begin collecting evidence.

Ask:

What false positives could affect this investigation? Consider same-name confusion, reused usernames, copied content, reposted media, machine translation errors, old archive captures, similar locations, and misleading timestamps.

Common false positives include:

• two people with the same name;
• two companies with similar names;
• usernames reused by unrelated people;
• old images reposted during a new event;
• AI-translated names that change meaning;
• archive captures that preserve a page after the relevant content changed;
• screenshots without original context;
• domains parked, transferred, or reused over time;
• social accounts impersonating an organization.

If you write these risks before searching, you are less likely to mistake a weak match for evidence.

Keep a Search Log

A search plan is not complete without a log.

The log should record both findings and failed searches. Failed searches matter because they show what was checked and prevent you from repeating the same path later.

Use a simple structure:

Search Question	Source / Query	Result	What It Supports	Limitation	Next Step
Is the domain connected to the organization?	Exact domain search	Found old press page	Possible public association	Page is archived, not current	Check archive dates
Was the video posted before the claimed event?	Reverse image/video search	Similar clip found earlier	Claim may be misleading	Need original upload	Search by caption
Is the username unique?	Cross-platform search	Same handle appears on two platforms	Possible connection	Could be unrelated user	Compare profile details

AI can format the log, summarize it, and identify gaps. But the content of the log must come from your checks.

Prompt:

Turn these investigation notes into a search log. Separate confirmed findings, weak indicators, failed searches, and open questions. Do not add facts that are not in the notes.

That final sentence protects the workflow.

Do not let AI complete the evidence for you.

Use AI as a Planning Assistant, Not a Source

AI can help you:

• rewrite vague questions;
• extract searchable objects;
• generate query layers;
• suggest source types;
• list false positives;
• structure a search log;
• identify missing checks;
• summarize what is still uncertain.

AI should not:

• invent sources;
• decide whether a claim is true;
• identify private people from weak signals;
• bypass privacy settings;

• scrape personal data at scale;
• turn correlation into attribution;
• replace primary source checks;
• write a confident conclusion from incomplete evidence.

The difference is simple.

Use AI before and after search, not instead of search.

Before search, it helps you plan.

After search, it helps you review gaps.

During verification, the evidence must come from sources you can inspect, document, and cite.

The Practical Workflow

Use this sequence before starting a new OSINT investigation:

1. Write the vague question.
2. Rewrite it as a precise investigative question.
3. Extract the searchable objects.
4. Choose the first object to investigate.
5. Build a search path for that object.
6. Generate query layers.
7. Identify source types.
8. List false positive risks.
9. Create a search log.

1. Start searching manually.
2. Record findings and failed searches.
3. Ask AI to review gaps, not to decide the conclusion.

This workflow is slower at the beginning.

That is the point.

A good search plan prevents wasted time later. It reduces random browsing, premature conclusions, repeated queries, and weak attribution. It also makes the final finding easier to defend because the path from question to evidence is visible.

OSINT is not only about finding information.

It is about knowing what kind of information would actually answer the question.

AI can help you build that plan.

The investigation still belongs to you.
Most OSINT mistakes do not begin with the wrong tool.

They begin before the tool is opened.

A researcher starts with a vague question, runs a few searches, saves random links, follows an interesting account, opens a map, checks a screenshot, asks an AI tool for suggestions, and suddenly the investigation has no shape. There are many fragments, but no plan.

The problem is not lack of effort.

The problem is that the search started before the question was operational.

AI can help at this stage. Not by finding the truth for you. Not by replacing search engines, archives, maps, registries, or primary sources. Its useful role is more basic: it can help you turn a vague investigative question into a structured search plan.

That plan should tell you what to look for, where to look, which words to test, which languages may matter, what evidence would count, and what risks could mislead you.

Before you investigate, build the search plan.

Start With the Real Question

Many investigations begin with a sentence that is too broad to search well.

Examples:

• Who is behind this website?
• Is this video real?
• Is this company connected to another company?
• Did this account post the original image?
• Is this claim about a protest accurate?
• Are these profiles controlled by the same person or organization?

These are reasonable questions, but they are not yet search plans.

The first step is to make the question more precise.

Instead of:

Who is behind this website?

write:

What public traces can connect this website to a person, organization, infrastructure, domain owner, social profile, company, or previous project?

Instead of:

Is this video real?

write:

Can the location, date, event, and original publication context of this video be independently checked?

This shift matters.

A broad question invites random searching. An operational question defines what can be checked.

AI can help you rewrite the question.

Prompt:

Turn this vague OSINT question into a precise investigative question. Separate what can be verified from what may remain uncertain. Question: [paste your question]

Do not accept the output automatically. Edit it until the question is specific enough to guide a

search.

Define the Objects of the Search

An OSINT search plan needs objects.

The object is the thing you are trying to examine: a domain, a username, an image, a video, a company, a location, a wallet, a document, a phone number, a public profile, an email address, a post, or a claim.

If you do not define the object, the search will expand too quickly.

Use a simple table:

Object	What It Is	What It May Reveal	Main Risk
Domain	Website address	infrastructure, archive history, related pages	privacy-protected registration
Username	Public handle	cross-platform activity, reused identity signals	false matches
Image	Visual file or screenshot	location, event, earlier versions	edited or cropped context
Company name	Legal or public entity	registries, officers, addresses, related firms	same-name confusion
Social post	Public claim or media	timeline, source, interaction network	deleted or reposted content

AI can help list the possible objects, especially when the case has several moving parts.

Prompt:

Extract the searchable objects from this case description. Group them by type: people, organizations, accounts, domains, media, locations, documents, technical indicators, and claims. For each object, explain what it may help verify and what false positive risk it creates. Case description: [paste your notes]

The goal is not to create a long list. The goal is to decide where the investigation should begin.

Build Search Paths, Not Just Search Queries

A query is one search.

A search path is a sequence.

For example, if the object is a domain, a search path may look like this:

1. Check the live website.
2. Save the URL and visible claims.
3. Search archived versions.
4. Compare old and current pages.
5. Check public domain and DNS information where available.
6. Search the domain in exact match.
7. Search unique page text.
8. Search connected emails, usernames, social links, or company names.
9. Record what each source supports.

If the object is a video, the path changes:

1. Preserve the original post.
2. Identify the earliest visible upload.
3. Extract visual clues.
4. Check location indicators.
5. Compare with maps, street-level imagery, or satellite imagery.
6. Check date clues such as weather, light, events, clothing, signage, or public reports.
7. Search for earlier versions of the same media.
8. Record what is confirmed, likely, or still unverified.

AI can suggest search paths, but you should adapt them to the case.

Prompt:

Create an OSINT search path for this object. Include the first sources to check, the order of checks, what each step can verify, what it cannot verify, and common false positives. Object: [domain / username / image / video / company / claim] Context: [short case description]

This is where AI becomes useful: it helps you avoid opening ten tabs before knowing why they matter.

Generate Queries in Layers

Good OSINT search is not one query. It is a set of query layers.

Start narrow.

Then expand.

Then translate.

Then search by related objects.

For a company or organization, query layers may include:

• exact name;
• exact name plus country or city;
• name plus director, founder, officer, grant, contract, sanction, lawsuit, procurement, partnership, domain;
• local-language spelling;
• abbreviations;
• former names;
• associated addresses;
• unique phrases from public pages;
• related domains or social handles.

For a social media claim, query layers may include:

• exact quote;
• key phrase without punctuation;
• platform-specific search;
• account handle;
• image or video caption;
• translated terms;
• date-limited searches;
• local media keywords;
• archived versions.

AI is good at generating query variations, especially across languages and spelling patterns.

Prompt:

Generate search query layers for this OSINT question. Include exact-match queries, broad discovery queries, local-language variations, date-based queries, and source-specific queries. Do not assume the claim is true. Question: [paste the question] Known objects: [paste objects] Likely countries/languages: [paste if known]

The last sentence is important: do not assume the claim is true.

Search queries can quietly reproduce the claim. If you search only for wording that confirms it, you may miss evidence that contradicts it.

Choose Source Types Before Collecting Links

An OSINT search plan should say which source types matter.

Otherwise, the investigation becomes a pile of links.

For identity or attribution questions, useful source types may include:

• official profiles;
• archived web pages;
• public company registries;
• domain and infrastructure records;
• public documents;
• conference pages;
• media interviews;
• social profile history;
• usernames reused across platforms.

For location questions:

• maps;
• street-level imagery;
• satellite imagery;
• public transport data;
• business listings;
• local news;
• weather records;
• public webcams, when legal and available;
• official event notices.

For timeline questions:

• original upload timestamp;
• archive timestamp;
• edited post history when visible;
• media reports;
• event calendars;
• weather and daylight clues;
• publication sequence across platforms.

AI can help build a source map.

Prompt:

Create a source map for this OSINT question. For each source type, explain what it can verify, what it cannot verify, and how reliable it may be. Question: [paste the question]

This prevents a common mistake: treating every link as equal.

A company registry, a reposted screenshot, a local article, a social media comment, and an archived page do not have the same evidentiary value. They may all be useful, but they support different parts of the analysis.

Add a False Positive Section

Every search plan should include a false positive section.

This is where AI can be especially useful because it can challenge your assumptions before you begin collecting evidence.

Ask:

What false positives could affect this investigation? Consider same-name confusion, reused usernames, copied content, reposted media, machine translation errors, old archive captures, similar locations, and misleading timestamps.

Common false positives include:

• two people with the same name;
• two companies with similar names;
• usernames reused by unrelated people;
• old images reposted during a new event;
• AI-translated names that change meaning;
• archive captures that preserve a page after the relevant content changed;
• screenshots without original context;
• domains parked, transferred, or reused over time;
• social accounts impersonating an organization.

If you write these risks before searching, you are less likely to mistake a weak match for evidence.

Keep a Search Log

A search plan is not complete without a log.

The log should record both findings and failed searches. Failed searches matter because they show what was checked and prevent you from repeating the same path later.

Use a simple structure:

Search Question	Source / Query	Result	What It Supports	Limitation	Next Step
Is the domain connected to the organization?	Exact domain search	Found old press page	Possible public association	Page is archived, not current	Check archive dates
Was the video posted before the claimed event?	Reverse image/video search	Similar clip found earlier	Claim may be misleading	Need original upload	Search by caption
Is the username	Cross-platform	Same handle	Possible	Could be	Compare profile

Search Question unique?	Source / Query search	Result appears on two platforms	What It Supports connection	Limitation unrelated user	Next Step details

AI can format the log, summarize it, and identify gaps. But the content of the log must come from your checks.

Prompt:

Turn these investigation notes into a search log. Separate confirmed findings, weak indicators, failed searches, and open questions. Do not add facts that are not in the notes.

That final sentence protects the workflow.

Do not let AI complete the evidence for you.

Use AI as a Planning Assistant, Not a Source

AI can help you:

• rewrite vague questions;
• extract searchable objects;
• generate query layers;
• suggest source types;
• list false positives;
• structure a search log;
• identify missing checks;
• summarize what is still uncertain.

AI should not:

• invent sources;
• decide whether a claim is true;
• identify private people from weak signals;
• bypass privacy settings;
• scrape personal data at scale;
• turn correlation into attribution;
• replace primary source checks;
• write a confident conclusion from incomplete evidence.

The difference is simple.

Use AI before and after search, not instead of search.

Before search, it helps you plan.

After search, it helps you review gaps.

During verification, the evidence must come from sources you can inspect, document, and cite.

The Practical Workflow

Use this sequence before starting a new OSINT investigation:

1. Write the vague question.
2. Rewrite it as a precise investigative question.
3. Extract the searchable objects.

4. Choose the first object to investigate.
5. Build a search path for that object.
6. Generate query layers.
7. Identify source types.
8. List false positive risks.
9. Create a search log.

1. Start searching manually.
2. Record findings and failed searches.
3. Ask AI to review gaps, not to decide the conclusion.

This workflow is slower at the beginning.

That is the point.

A good search plan prevents wasted time later. It reduces random browsing, premature conclusions, repeated queries, and weak attribution. It also makes the final finding easier to defend because the path from question to evidence is visible.

OSINT is not only about finding information.

It is about knowing what kind of information would actually answer the question.

AI can help you build that plan.

The investigation still belongs to you.