Storm Quick Reference - Example Pivots and Traversals

Type	Explicit Syntax Required?	Examples - Implicit syntax (no need to specify source / target props) - Explicit syntax (specifies source & target props)	Query / Question
Pivot Out (->)			
Primary to secondary property	N	`inet:fqdn=vertex.link -> inet:dns:a` `inet:fqdn=vertex.link -> inet:dns:a:fqdn`	For the FQDN vertex.link, **show me its DNS A records**
Secondary to primary property	N	`inet:dns:a:fqdn=vertex.link -> inet:ipv4` `inet:dns:a:fqdn=vertex.link :ipv4 -> inet:ipv4`	For the DNS A records for vertex.link, **show me the associated IPv4 addresses**
Wildcard - from **all** secondary properties to **all** associated nodes	N	`file:bytes#cno.mal.redtree -> *` `n/a`	For files associated with the 'redtree' malware family, **show me all the things those files reference ("point to")** (will pivot from the file(s) to things like associated hashes, file paths (from PDB paths), etc.
Secondary to secondary property	**Y**	`n/a` `inet:dns:a:fqdn=vertex.link :ipv4 -> inet:dns:a:ipv4`	For the DNS A records for vertex.link, **show me other DNS A records that resolve to the same IPv4 addresses**
Between properties of different types	**Y**	`n/a` `file:path=c:\temp\evil.exe -> it:dev:regval:str`	For the file path c:\temp\evil.exe, **show me all of the Windows registry values that contain this path**
Pivot Out and Join (-+>) - Same as a pivot out operation, but **retains** the source nodes and **combines** them with the target nodes in the results			
Any pivot out	Depends on pivot	`inet:dns:a:fqdn=vertex.link -+> inet:ipv4`	For the DNS A records for vertex.link, **show me both the A records AND the associated IPv4 addresses**

Pivot In (<- *) - "Pivot in" is a special use case and can only be used with a wildcard (*).		
Wildcard - from the node to **all** nodes where the node is a secondary property	`inet:email=lnarmetov@mail.ru <- *`	For the email 'lnarmetov@mail.ru', **show me all the things that reference ("point to") that email** (will pivot from the email to nodes that contain the email, such as WHOIS records, contact records, SOA records, etc.)

Pivot to / from Tags			
Type	**Operator**	**Example**	**Query / Question**
Pivot to tags	`-> #`	`inet:fqdn=wifb.site -> #` `#cno.mal.redtree -> #`	Show me **all the tags (syn:tag nodes)** on the FQDN wifb.site Show me **all the tags on all the nodes** tagged #cno.mal.redtree
Pivot from tags	`<syn:tag> -> *` `<syn:tag> -> <form>`	`syn:tag=rep.feye.apt29 -> *` `syn:tag=rep.feye.apt29 -> inet:fqdn`	Show me **all the things FireEye associates with APT29** Show me **the FQDNs FireEye associates with APT29**

Traverse ("walk") Lightweight (Light) Edge - Can be traversed in either direction; can be combined with **join** (`-(<edge>)+>` or `<+(<edge>)-`)			
Traverse named edge(s)	`-(<edge>)>` `<(<edge>)-`	`media:news:org=eset -(refs)> inet:fqdn` `inet:fqdn=evil.com <((refs,seen))- *`	For articles published by ESET, **show me all the FQDNs they reference** For FQDN evil.com, **show me anything it is linked to by a 'refs' or 'seen' edge**
Traverse any edges	`-(*)>` `<(*)-`	`inet:ipv4=84.38.183.45 <(*)- *`	For IPv4 84.38.183.45, **show me anything it is linked to by any edge**

Pivot and Traverse - Combines property pivots and edge traversals			
Pivot and walk out	`-->`	`media:news:org=eset --> *`	For all articles published by ESET, show me all the things **the articles reference or link to using any edge**
Pivot and walk in	`<--`	`inet:ipv4=84.38.183.45 <-- *`	For IPv4 address 84.38.183.45, show me all the things that **reference this IP or are linked to it using any edge**

For a complete list of Storm pivot operators and additional examples, see the Pivoting section of the Storm Reference Guide.