Info Gathering

Obiettivo: Effettuare la simulazione di fase di Raccolta Informazioni su un Target a Scelta.
Strumenti Utilizzati:

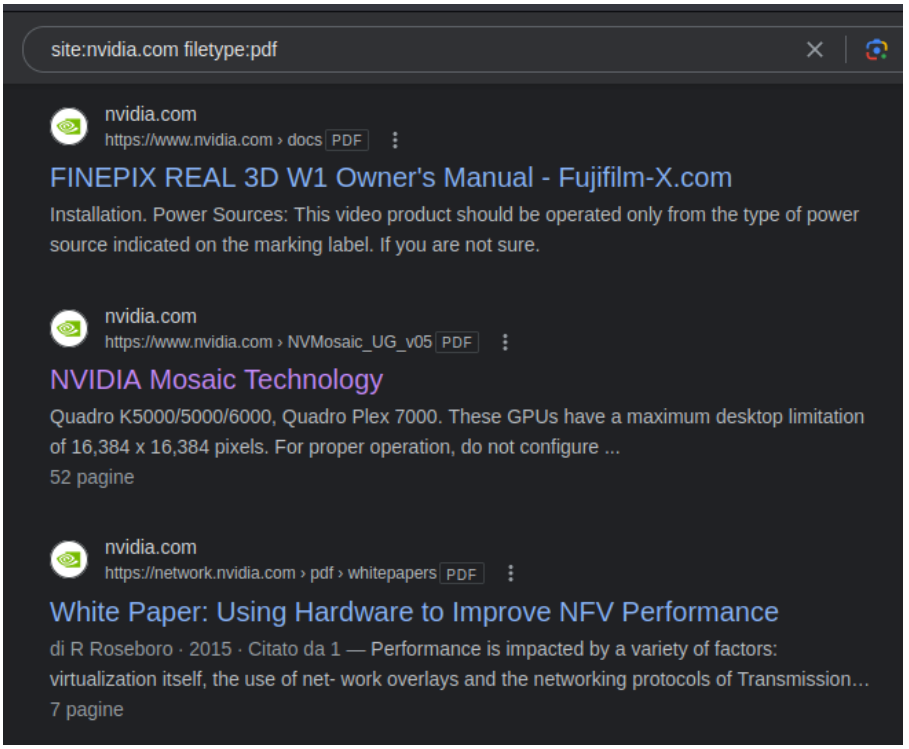
- Motore di Ricerca Google
- DMitry/1.3 a (Unix)
- Recon-ng 5.1.2
- Maltego 4.4.1

1) Scelta del Bersaglio e inizio della Raccolta di Informazioni

Per cominciare ho scelto come bersaglio *l'Azienda Internazionale Nvidia* sviluppatrice di processori grafici per il mercato videoludico e professionale e non solo. Come primo strumento per la raccolta ho usato il motore di ricerca di Google sfruttando alcuni dei suoi operatori tra i quali: **site - filetype - cache - intitle**
Con **site** ho cercato informazioni generiche sull'azienda in questione oltre a possibili sottodomini. Questo serve anche a conoscere il probabile perimetro dell'esposizione sul web del bersaglio. Nel nostro caso Nvidia è più esposta sul web ma si suppone che abbia anche le dovute misure di sicurezza.

Altri Operatori che ho utilizzato sono:

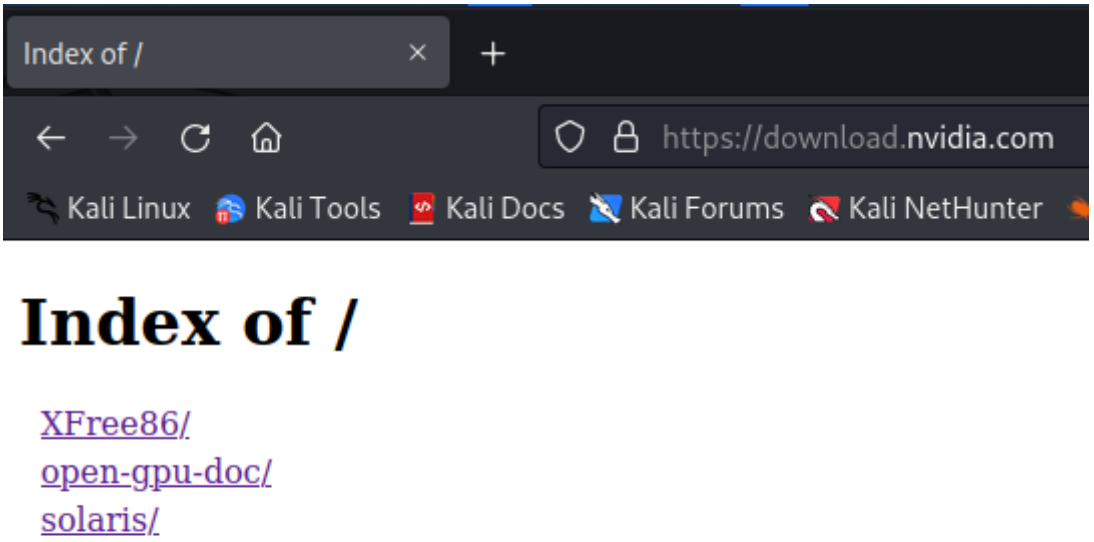
filetype: per cercare file di un determinato formato (ho cercato pdf perchè il più diffuso oltre a docx)



cache: grazie a questo operatore posso ricercare la cache della pagina che mi serve, nel caso fosse momentaneamente offline, per poter studiare il codice sorgente per esempio


```
<!DOCTYPE HTML>
<html class="html-page no-js" xmlns="http://www.w3.org/1999/xhtml" lang="en-us" xml:lang="en-us">
    <head>



<meta http-equiv="X-UA-Compatible" content="IE=edge"/>
<meta name="robots" content="NOODP,NOYDIR"/>
<meta name="viewport" content="width=device-width, initial-scale=1"/>
<meta http-equiv="content-type" content="text/html; charset=UTF-8"/>
<meta name="keywords" content="gpu, graphics card, gaming, high performance computing, autonomous vehicles, robotics, nvidia"/>
<meta name="description" content="NVIDIA invents the GPU and drives advances in AI, HPC, gaming, creative design, autonomous vehicles, and robotics."/>
<meta name="nv-pub-date" content="2023-05-30T04:19:21.000Z"/>


<meta property="og:site_name" content="NVIDIA"/>
<meta property="og:type" content="website"/>
<meta property="og:url" content="https://www.nvidia.com/en-us/"/>
<meta property="og:title" content="World Leader in AI Computing"/>
<meta property="og:description" content="We create the world's fastest supercomputer and largest gaming platform."/>

        <meta property="og:image" content="https://www.nvidia.com/content/dam/en-zz/Solutions/homepage/v2/sfg/nvidia-corporate-og-image-1200x630.jpg"/>



<meta name="twitter:card" content="summary_large_image"/>
<meta name="twitter:site" content="@NVIDIA"/>
<meta name="twitter:creator" content="@NVIDIA"/>
<meta name="twitter:title" content="World Leader in Artificial Intelligence Computing"/>
<meta name="twitter:url" content="https://www.nvidia.com/en-us/"/>
<meta name="twitter:description" content="NVIDIA invents the GPU, creates the largest gaming platform, powers the world's fastest supercomputer, and drives advance
```

intitle: ho usato principalmente questo operatore per cercare possibili *Directory listing* trovando però solo una serie di download probabilmente di driver Nvidia disponibili gratuitamente



2) **DMitry**

Successivamente per trovare informazioni più specifiche.
Indirizzi email: molto generici come “privacy” e “cudatool”, toolkit per developer

```
┌──(root㉿kali)-[/home/kali]
└─# dmitry -e www.nvidia.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:2.21.14.59
HostName:www.nvidia.com

Gathered E-Mail information for nvidia.com
------------------------------------
Searching Google.com:80...
privacy@nvidia.com
nvdla@nvidia.com
isharif@nvidia.com
adamt@nvidia.com
dnellans@nvidia.com
cudatools@nvidia.com
Searching Altavista.com:80 ...
Found 6 E-Mail(s) for host nvidia.com, Searched 0 pages containing 0 results

All scans completed, exiting
```

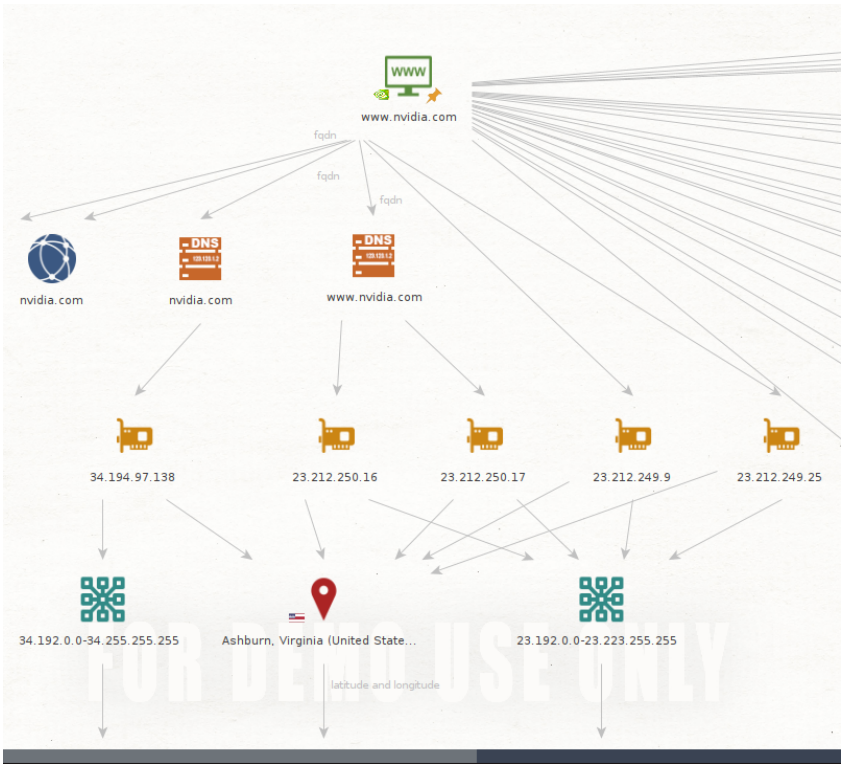
NB: In questo caso ho usato lo *switch* **-e** per cercare nello specifico gli indirizzi email, nella successiva non ho usato switch ma ho ritagliato i sottodomini trovati.

Sottodomini: più interessante è la scoperta dei vari sottodomini di Nvidia.com. Per un attaccante potrebbero essere più appetibili per accedere a informazioni di brevetti, dei developer dell'azienda o i loro dati personali

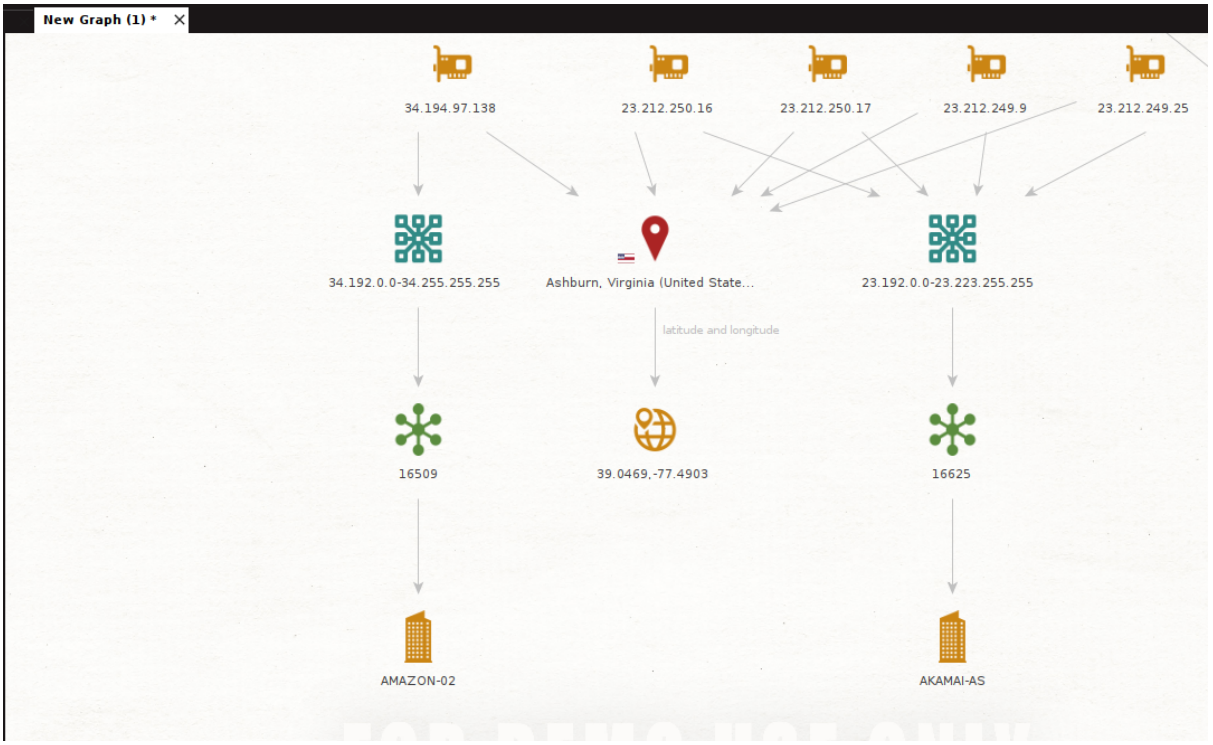
```
Gathered Netcraft information for www.nvidia.com
------------------------------------------

Retrieving Netcraft.com information for www.nvidia.com
Netcraft.com Information gathered

Gathered Subdomain information for nvidia.com
------------------------------------------

Searching Google.com:80 ...
HostName:www.nvidia.com
HostIP:195.22.200.66
HostName:store.nvidia.com
HostIP:195.22.200.66
HostName:developer.nvidia.com
HostIP:152.199.20.126
HostName:nvidianews.nvidia.com
HostIP:35.190.66.32
HostName:blogs.nvidia.com
HostIP:152.195.53.224
HostName:docs.nvidia.com
HostIP:2.21.14.59
HostName:catalog.ngc.nvidia.com
HostIP:44.232.50.28
HostName:investor.nvidia.com
HostIP:162.159.129.11
HostName:devtalk.nvidia.com
HostIP:184.105.99.75
HostName:nvid.nvidia.com
HostIP:68.232.34.75
HostName:x3ewww.nvidia.com
HostIP:127.0.0.1
Searching Altavista.com:80 ...
Found 11 possible subdomain(s) for host nvidia.com, Searched 0 pages containing 0 results
```

3) Maltego

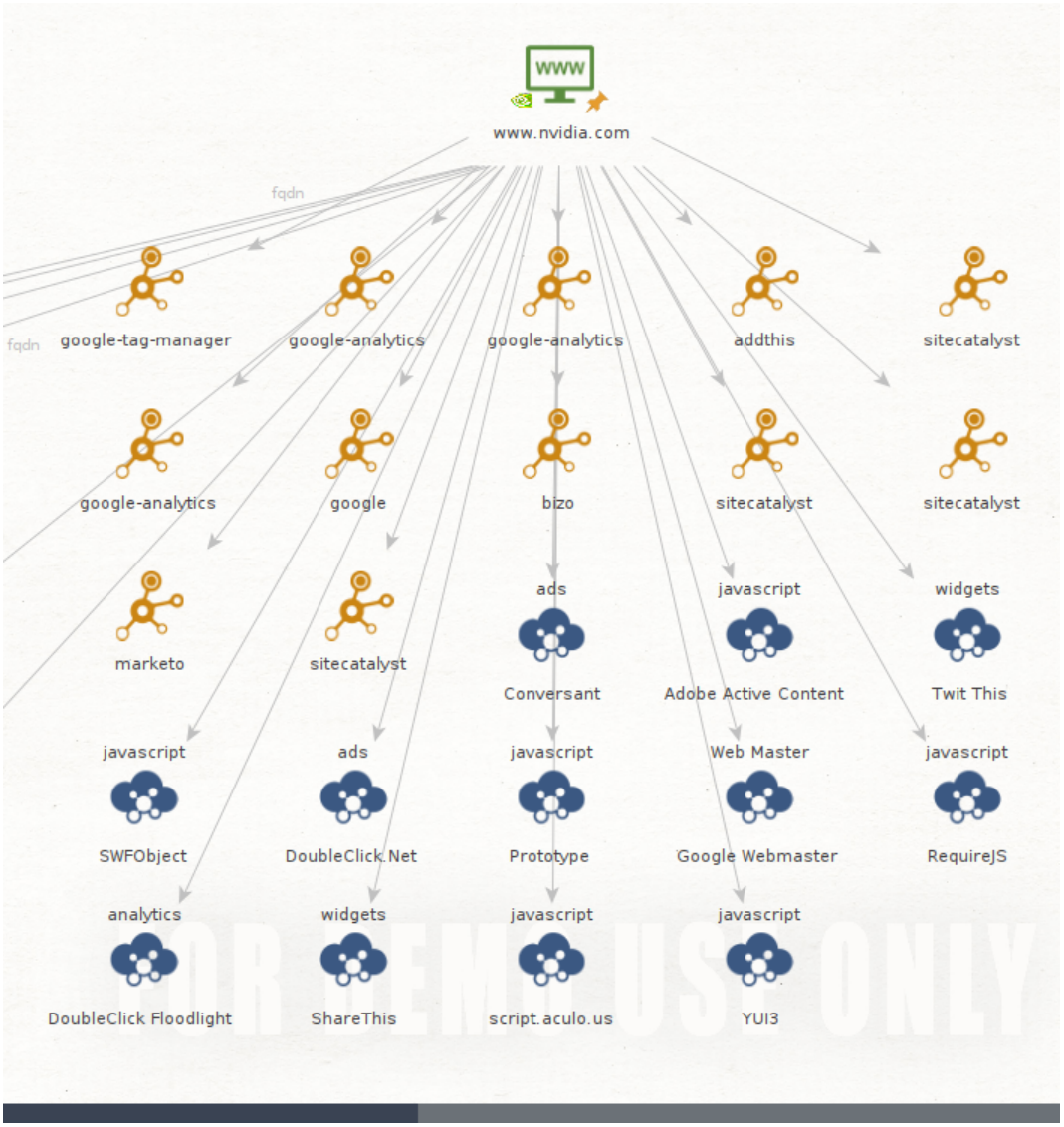
Maltego è un programma più complesso rispetto a Dmitry, ma decisamente più completo. Partendo dal sito web www.nvidia.com ho potuto cercare ogni tipo di informazione che il programma mi permetteva grazie a quelle che sono chiamate "trasformate".



Dal sito Web ho trovato il **Dominio**, i **DNS** e degli **Indirizzi IP**. Ho cercato la location di questi ultimi insieme ad altri indirizzi IP derivanti dai Server DNS e ho potuto constatare che sono tutti situati (fisicamente) in **Virginia negli Stati Uniti**. Ho potuto anche ricercare quelli che sono **Netblocks**, ovvero range di **Indirizzi IP**.



Da questi **Netblocks** sono potuto alla fine risalire a quali compagnie appartengono questi Server che offrono il loro utilizzo come servizio ad Nvidia.com, Amazon e Akamai (azienda che fornisce una piattaforma per la distribuzione di contenuti via Internet).



Nel voler utilizzare ulteriormente Maltego ho esteso la ricerca non solo alle precedenti trasformate ma anche ad altre come “**Technology**” e “**Relationship**”. Le prime vanno ad indicare quale tipo di tecnologia utilizza il sito di Nvidia come vari tipi di *javascript*, la seconda è legata probabilmente a siti che monitorano Nvidia.com forse per indagini di mercato essendo presente *Google Analytics*.