

**TUGAS KEAMANAN JARINGAN KOMPUTER
TAHAP RECONNAISSANCE**



DISUSUN OLEH:

NAMA : Fahrul Rozi

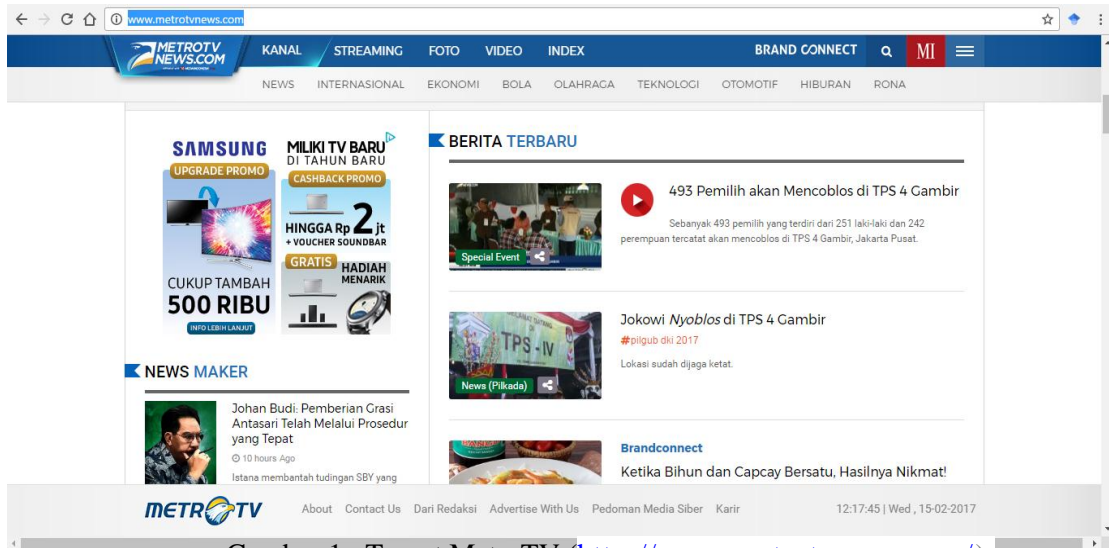
NIM : 0901181320022

**JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA**

2017

Tahap Reconnaissance

Pada tugas pertama keamanan jaringan komputer yaitu melakukan tahap reconnaissance. Pada tahap ini penulis mengumpulkan data sebanyak-banyaknya sebelum melakukan hacking pada target. Target pada tugas ini adalah MetroTV (<http://www.metrotvnews.com/>). MetroTV adalah sebuah stasiun televisi swasta berita yang berkedudukan di Indonesia. MetroTV didirikan oleh PT Media Televisi Indonesia, resmi mengudara sejak 25 November 2000 di Jakarta.

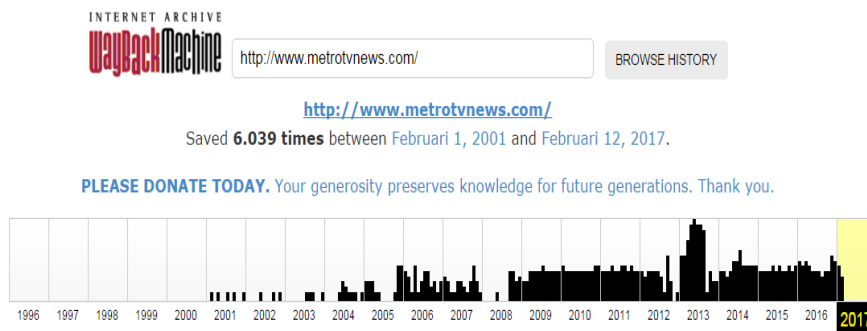


Gambar 1 : Target MetroTV (<http://www.metrotvnews.com/>).

Berikut adalah data yang dapat disajikan bersangkutan dengan target :

1. Tools web.archive.org

Pada tools ini data yang didapatkan yaitu menunjukkan bahwa MetroTV mulai menggunakan domain metrotvnews.com pada tahun 2001 dan terus melakukan update secara rutin hingga saat ini seperti pada gambar grafik yang ditunjukkan pada gambar 2 Dibawah ini.



Gambar 1.1 : Browse Histori MetroTV

Peningkatan atau update pada web ini sangatlah penting dikarenakan untuk pemeliharaan server dan memperbaiki tampilan agar lebih menarik serta menampilkan berita yang terbaru.


2. Tools toolbar.netcraft.com

Data dari tools ini didapatkan bahwa target dari Metro TV memiliki ip address 103.225.66.90 dengan domain metrotvnews.com serta network owner dari PT Media Televisi Indonesia ,nameserver ns1.metrotvnews.com dan dns admin nya menggunakan sysadmin@metrotvnews.com. Informasi tersebut dapat ditunjukkan pada gambar

Background

Site title	Not Present	Date first seen	May 2000
Site rank	119611	Primary language	Unknown
Description	Not Present		
Keywords	Not Present		

Network

Site	http://www.metrotvnews.com	Netblock Owner	PT Media Televisi Indonesia
Domain	metrotvnews.com	Nameserver	ns1.metrotvnews.com
IP address	103.225.66.90	DNS admin	sysadmin@metrotvnews.com
IPv6 address	Not Present	Reverse DNS	ip66-90.metrotvnews.com
Domain registrar	unknown	Nameserver organisation	unknown
Organisation	unknown	Hosting company	metrotvnews.com
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	unknown
Hosting country	 ID		

Gambar 2.1 : informasi MetroTV

Selain itu tools netcraft ini dapat menampilkan hosting history yang dikeluarkan oleh netblock owner dari MetroTV hal tersebut dapat dilihat pada gambar 3.1 ,serta ip address , OS, layanan web server dan waktu penghostingan .

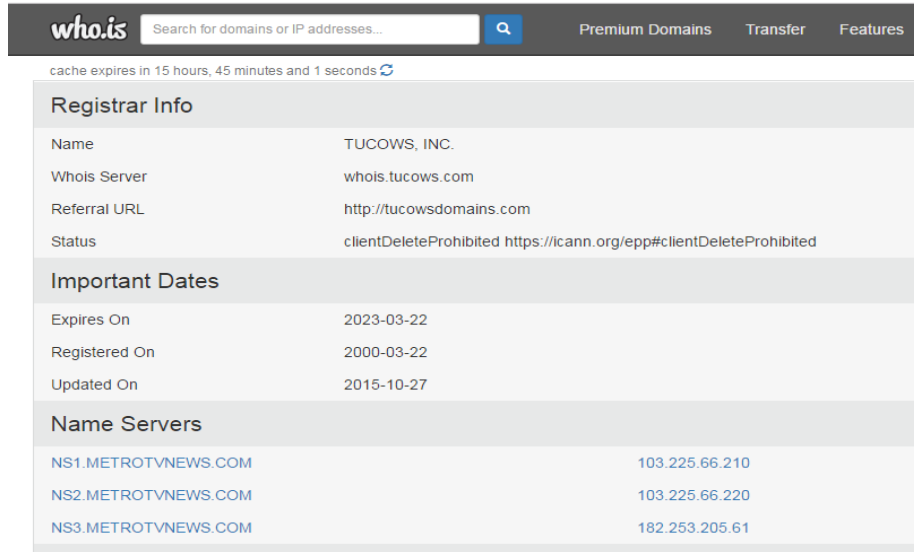
Hosting History

Netblock owner	IP address	OS	Web server	Last seen
PT Media Televisi Indonesia Corporate / Direct Member IDNIC Jl. Pilar Mas Raya Kav.A-D Kedoya Kebon Jeruk, Jakarta 11015.	103.225.66.90	Linux	nginx	15-Jan-2017
PT Media Televisi Indonesia Corporate / Direct Member IDNIC Jl. Pilar Mas Raya Kav.A-D Kedoya Kebon Jeruk, Jakarta 11015.	103.225.66.90	Linux	nginx/1.6.0	26-Oct-2014
PT Media Televisi Indonesia Corporate / Direct Member IDNIC Jl. Pilar Mas Raya Kav.A-D Kedoya Kebon Jeruk, Jakarta 11015.	103.225.66.90	Linux	nginx/1.2.6 Ubuntu	15-Jul-2014
Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.22	Linux	Apache/2.2.15 CentOS	12-Feb-2014
Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.22	Linux	Apache/2.2.3 CentOS	7-Mar-2012
Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.22	Linux	Apache/2.2.3 Red Hat	30-Jul-2011
Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.22	Linux	Apache/2.2.3 CentOS	2-May-2009
Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.22	Windows Server 2003	Microsoft-IIS/6.0	25-Jul-2008
Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.158	Windows Server 2003	Microsoft-IIS/6.0	27-Jun-2005
Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.158	Windows 2000	Microsoft-IIS/5.0	21-Apr-2005

Gambar 2.2 : MetroTV Hosting history

3. Tools who.is dan whois.domaintools.com

Informasi yang didapat dari tools who.id dan whois.domaintools.com ini sebenarnya hampir sama yakni menampilkan informasi- informasi dari MetroTV seperti register info : nama `tucows.inc` , important date : expired on 2013-03-22, register on 2000-03-22, update on 2015-10-27. Selain itu , dengan menggunakan kedua tools ini kita dapat mengetahui informasi tentang name server yang digunakan dan data register. MetroTV menggunakan lebih dari satu name server dan register data. Informasi-informasi tersebut dapat dilihat pada gambar 3.sub.



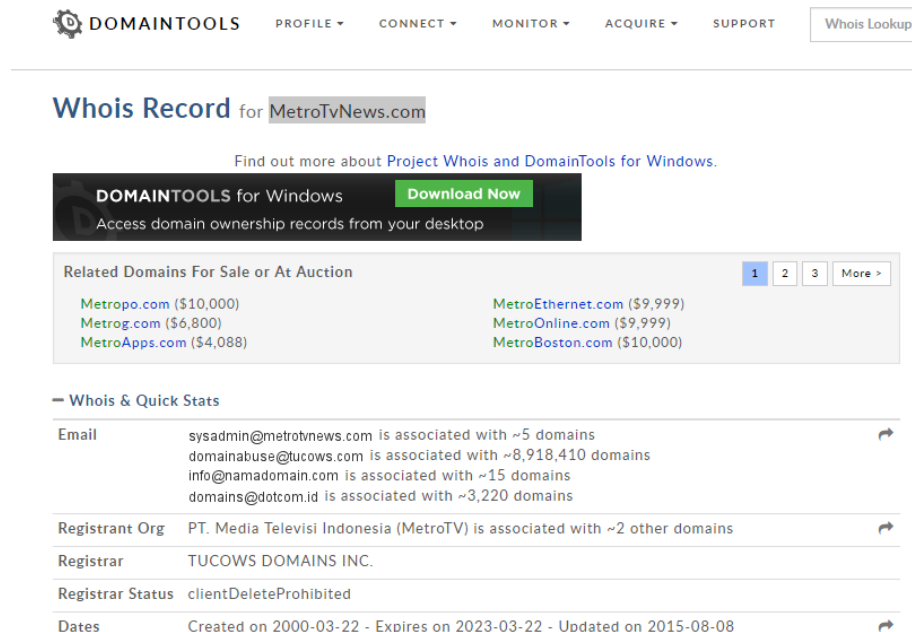
The screenshot shows the who.is website interface. At the top, there is a search bar with the text "Search for domains or IP addresses...". To the right of the search bar are links for "Premium Domains", "Transfer", and "Features". Below the search bar, a message states "cache expires in 15 hours, 45 minutes and 1 seconds". The main content is divided into three sections: "Registrar Info", "Important Dates", and "Name Servers".

Registrar Info	
Name	TUCOWS, INC.
Whois Server	whois.tucows.com
Referral URL	http://tucowsdomains.com
Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited

Important Dates	
Expires On	2023-03-22
Registered On	2000-03-22
Updated On	2015-10-27

Name Servers	
NS1.METROTVNEWS.COM	103.225.66.210
NS2.METROTVNEWS.COM	103.225.66.220
NS3.METROTVNEWS.COM	182.253.205.61

Gambar 3.1 : Informasi MetroTV menggunakan who.is



The screenshot shows the whois.domaintools.com website interface. At the top, there is a navigation menu with links for "PROFILE", "CONNECT", "MONITOR", "ACQUIRE", and "SUPPORT". A "Whois Lookup" button is also visible. The main content is titled "Whois Record for MetroTvNews.com". Below the title, there is a promotional banner for "DOMAINTOOLS for Windows" with a "Download Now" button. The banner text reads "Access domain ownership records from your desktop". Below the banner, there is a section titled "Related Domains For Sale or At Auction" with a list of domains and their prices: Metropo.com (\$10,000), Metrog.com (\$6,800), MetroApps.com (\$4,088), MetroEthernet.com (\$9,999), MetroOnline.com (\$9,999), and MetroBoston.com (\$10,000). Below this section, there is a "Whois & Quick Stats" section with a table of domain-related information.

Whois & Quick Stats	
Email	sysadmin@metrotvnews.com is associated with ~5 domains domainabuse@tucows.com is associated with ~8,918,410 domains info@namadomain.com is associated with ~15 domains domains@dotcom.id is associated with ~3,220 domains
Registrant Org	PT. Media Televisi Indonesia (MetroTV) is associated with ~2 other domains
Registrar	TUCOWS DOMAINS INC.
Registrar Status	clientDeleteProhibited
Dates	Created on 2000-03-22 - Expires on 2023-03-22 - Updated on 2015-08-08

Gambar 3.2 : Informasi MetroTV menggunakan whois.domaintools.com

who.is Search for domains or IP addresses... Premium Domains Transfer Features

Registrar Data Make Private

Registrant Contact Information:

Name	System Administrator
Organization	PT. Media Televisi Indonesia (MetroTV)
Address	Pilar Mas Raya Kav. A-D Kedoya, Kebon Jeruk
City	Jakarta Barat
State / Province	DKI Jakarta
Postal Code	11520
Country	ID
Phone	+62.2158300077
Fax	+62.215816151
Email	sysadmin@netrotvnews.com

Administrative Contact Information:

Name	System Administrator
Organization	PT. Media Televisi Indonesia (MetroTV)
Address	Pilar Mas Raya Kav. A-D Kedoya, Kebon Jeruk
City	Jakarta Barat
State / Province	DKI Jakarta
Postal Code	11520
Country	ID
Phone	+62.2158300077
Fax	+62.215816151
Email	sysadmin@netrotvnews.com

Technical Contact Information:

Name	System Administrator
Organization	PT. Media Televisi Indonesia (MetroTV)
Address	Pilar Mas Raya Kav. A-D Kedoya, Kebon Jeruk
City	Jakarta Barat
State / Province	DKI Jakarta
Postal Code	11520
Country	ID
Phone	+62.2158300077
Fax	+62.215816151
Email	sysadmin@netrotvnews.com

Gambar 3.3 : Register data menggunakan who.is

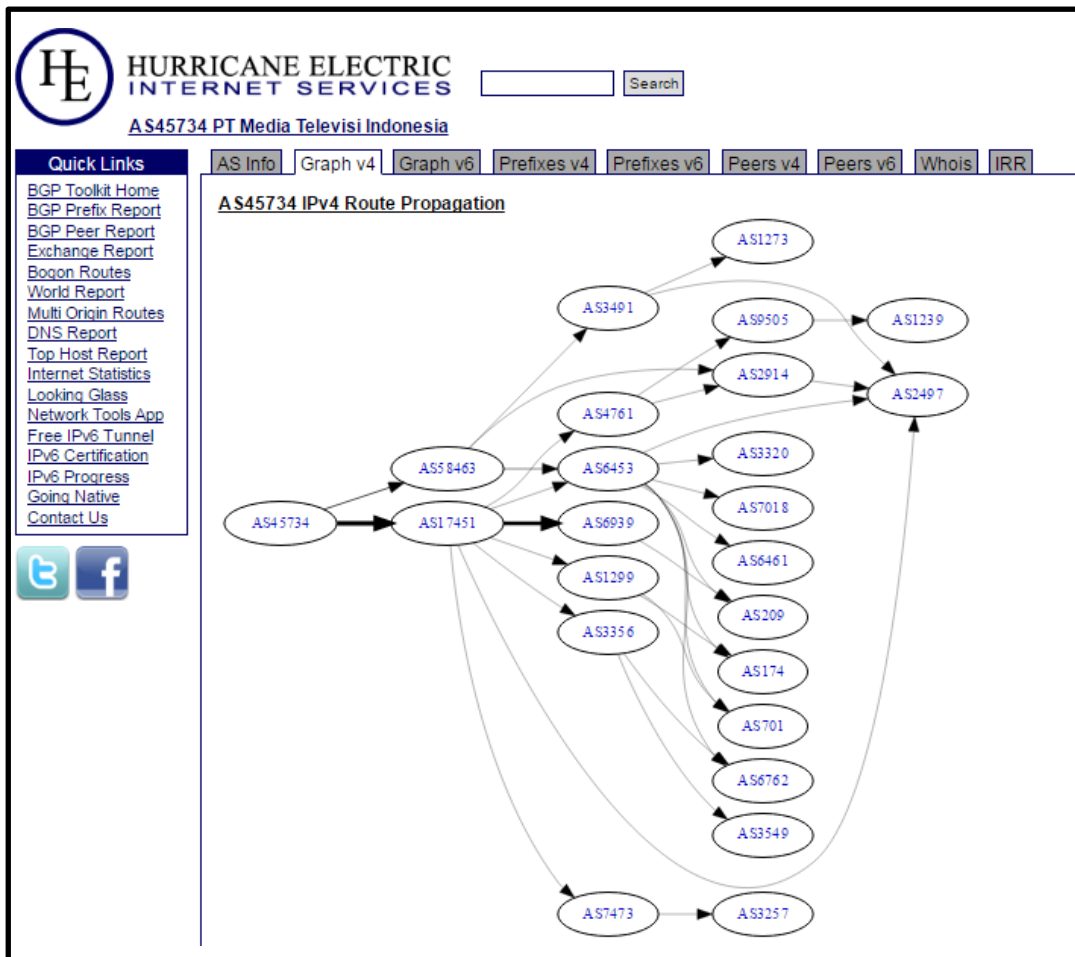
Yang membedakan kedua tools ini yaitu dapat dilihat pada gambar 3.4 dengan tools whois.domaintools.com terdapat AS Number .ASN dari MetroTV ini adalah **AS45734**. ASN ini merupakan kumpulan routing internet protocol yang terkoneksi dibawah naungan satu atau lebih operator jaringan untuk kepentingan satu entitas register atou domain yang diberikan secara umum yang mendefinisikan routing policy ke dalam internet. Pada gambar 3.4 ini juga terdapat informasi tentang website MetroTV terbaru atau telah di update.

Dates	Created on 2000-03-22 - Expires on 2023-03-22 - Updated on 2015-08-08	↗
Name Server(s)	NS1.METROTVNEWS.COM (has 4 domains) NS2.METROTVNEWS.COM (has 4 domains) NS3.METROTVNEWS.COM (has 4 domains)	↗
IP Address	103.225.66.90 - 3 other sites hosted on this server	↗
IP Location	🇮🇩 - Jakarta Raya - Jakarta - Pt Media Televisi Indonesia	
ASN	🇮🇩 AS45734 IDNIC-METROTV-AS-ID PT Media Televisi Indonesia, ID (registered Apr 06, 2009)	
Whois History	805 records have been archived since 2000-11-23	↗
IP History	7 changes on 4 unique IP addresses over 12 years	↗
Registrar History	2 registrars	↗
Hosting History	9 changes on 5 unique name servers over 13 years	↗
Whois Server	whois.tucows.com	
— Website		
Website Title	🌐 Metrotvnews.com: News Video Portal	Visit Website ↗
Server Type	nginx	
Response Code	200	
SEO Score	81%	
Terms	2135 (Unique: 954, Linked: 1295)	
Images	160 (Alt tags missing: 15)	
Links	585 (Internal: 450, Outbound: 9)	

Gambar 3.4 : Informasi ASN MetroTV menggunakan whois.domaintools.com

4. Tools bgp.he.net

Bicara tentang AS Number , Tools bgp.he.net dapat menampilkan AS Number dari target .Berikut ini merupakan informasi yang dapat menampilkan route propagation dari AS Number MetroTV / PT Media Televisi Indonesia **AS45734**dapat dilihat pada gambar 4.1.



Gambar 4.1 : AS45734 IPv4 Route Propagation