

Netzwerk-Forensik

Jens Berger
Lehrgebiet Datennetze



*“Network forensics is a **sub-branch of digital forensics** relating to the **monitoring and analysis of computer network traffic** for the purposes of information gathering, legal evidence, or intrusion detection. Unlike other areas of digital forensics, network investigations deal with **volatile and dynamic information**. Network traffic is transmitted and then lost, so network forensics is often a **pro-active investigation**.”*


- Teilgebiet der IT-Forensik
- Überwachung & Analyse von Netzwerkverkehr
- Flüchtige und dynamische Daten
- Proaktives Verfahren

- Malware verrät sich im Netzwerk
- Orten von Netzangriffen
- Internen Angriff aufdecken
- Genaue Rekonstruktion von Vorfällen
- Prävention und Gegenmaßnahmen
- Integre Daten

- Methoden der Netzwerk-Forensik untersuchen
- Anwendung dieser Methoden an Beispielszenarien
- Analyse und Prävention von Malware
- Netzwerk auf Angriffe vorbereiten
- Best Practice

- Plug-in für Browser
 - Ignoriert Wartezeit und Geschwindigkeitslimit
 - Einsatz: unbegrenzt Videos gucken auf kinox.to

Start sharing your videos [Upload](#) ... and make money!




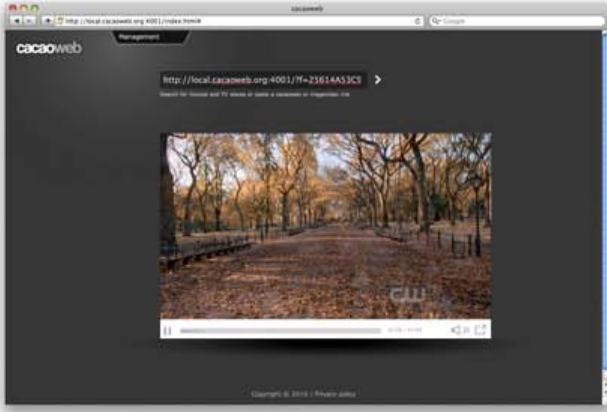
CacaoWeb

Version 1.2

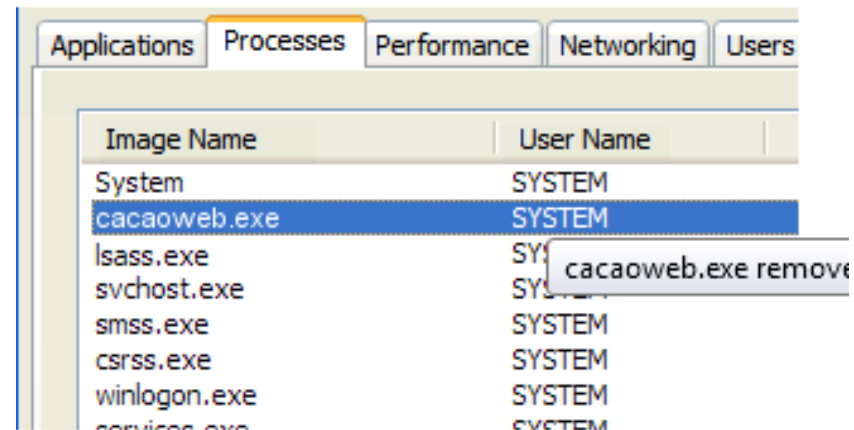
cacaoweb is a free plugin to watch, share and host videos and files online in streaming. Try now!

- Watch your favorite movies and TV shows in streaming
- Upload and share your files and videos with the world
- Get rid of time limits, like with megavideo, videobb, videozer, etc.

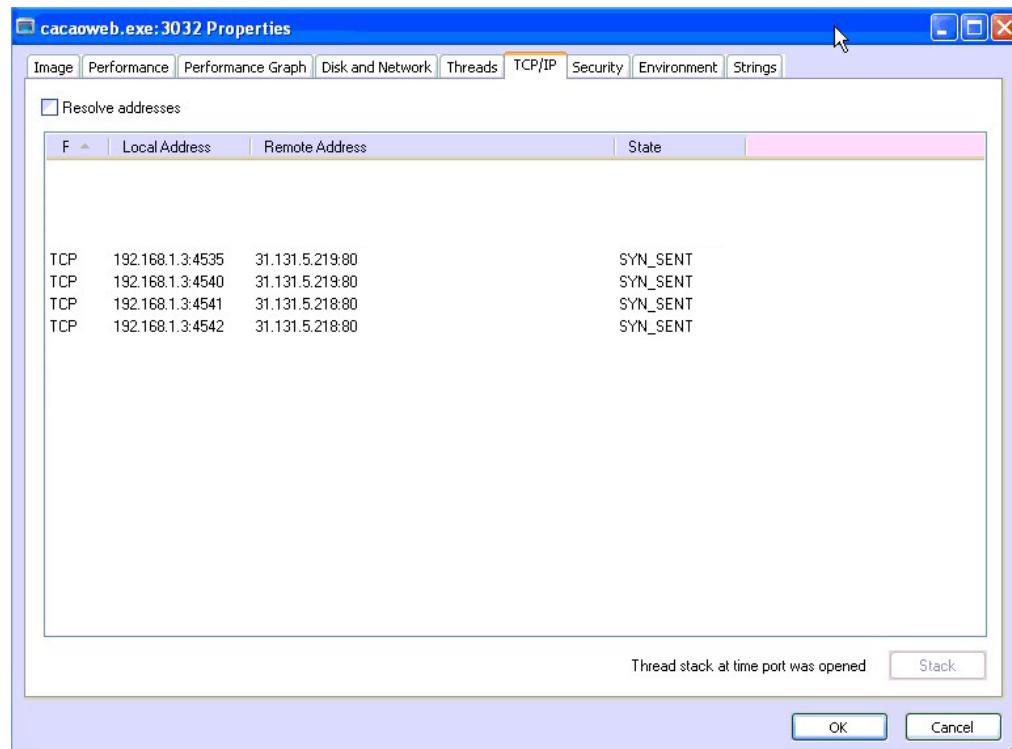
[Download](#) 



- Nach der Installation:
 - Befindet sich im Autostart
 - Prozess ohne sichtbares Fenster
 - Ansonsten nichts Auffälliges

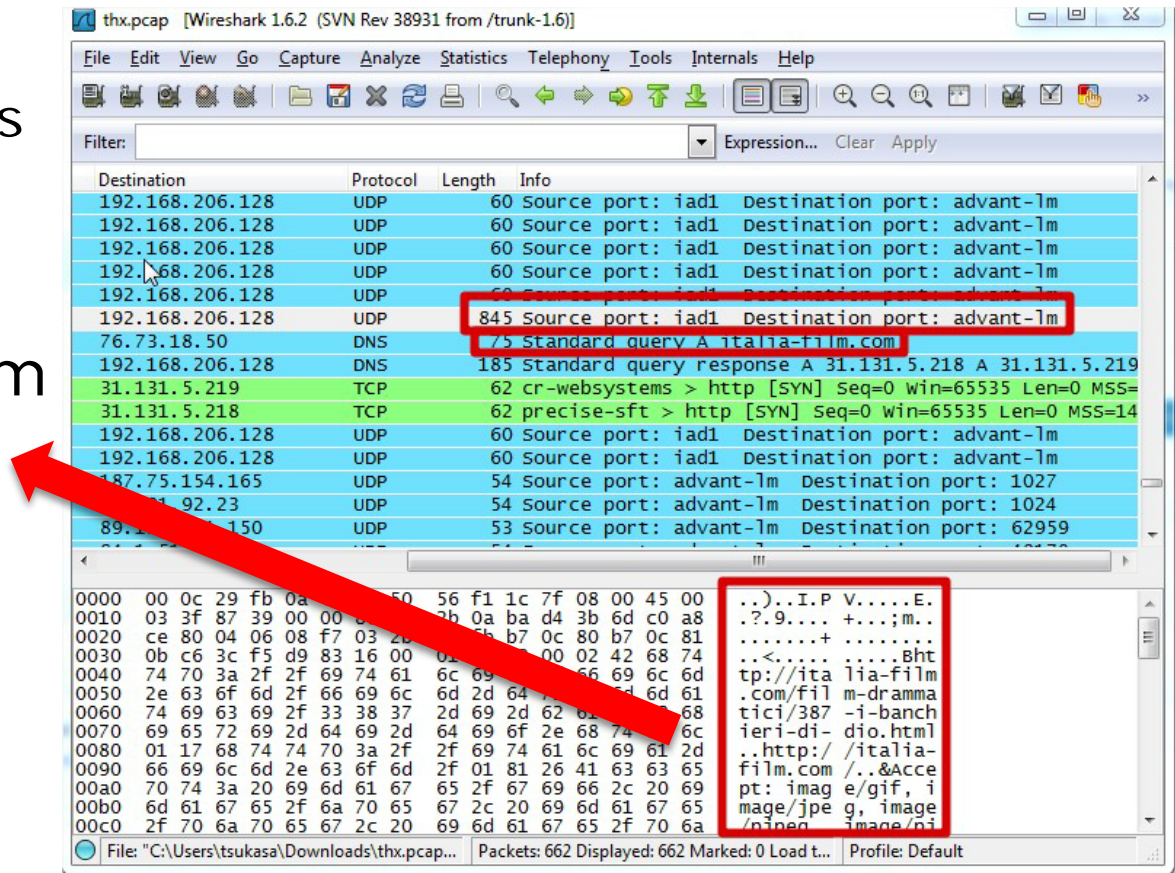


- Netzwerk-Überprüfung:
 - Öffnet Ports
 - Stellt eine Internetverbindung her



- Genauere Analyse per Wireshark
 - Führt UDP-Flood Attacken durch
 - Malware
 - Teil eines Botnetzes

■ Ziel: italia-film.com



The screenshot shows a Wireshark capture of network traffic. The packet list pane displays several UDP packets from source IP 192.168.206.128 to destination IP 192.168.206.128 on port 845. A red box highlights one of these packets. Below it, a DNS query for 'italia-film.com' is visible, also highlighted with a red box. A red arrow points from the text 'Ziel: italia-film.com' to the DNS query. The packet details pane shows the structure of the DNS query, including the question section with the query name 'italia-film.com'.

Destination	Protocol	Length	Info
192.168.206.128	UDP	60	Source port: iad1 Destination port: advant-1m
192.168.206.128	UDP	60	Source port: iad1 Destination port: advant-1m
192.168.206.128	UDP	60	Source port: iad1 Destination port: advant-1m
192.168.206.128	UDP	60	Source port: iad1 Destination port: advant-1m
192.168.206.128	UDP	60	Source port: iad1 Destination port: advant-1m
192.168.206.128	UDP	845	Source port: iad1 Destination port: advant-1m
76.73.18.50	DNS	75	Standard query A italia-film.com
192.168.206.128	DNS	185	Standard query response A 31.131.5.218 A 31.131.5.219
31.131.5.219	TCP	62	cr-websystems > http [SYN] Seq=0 win=65535 Len=0 MSS=
31.131.5.218	TCP	62	precise-sft > http [SYN] Seq=0 win=65535 Len=0 MSS=14
192.168.206.128	UDP	60	Source port: iad1 Destination port: advant-1m
192.168.206.128	UDP	60	Source port: iad1 Destination port: advant-1m
187.75.154.165	UDP	54	Source port: advant-1m Destination port: 1027
89.23.1.92.23	UDP	54	Source port: advant-1m Destination port: 1024
89.23.1.150	UDP	53	Source port: advant-1m Destination port: 62959

- Mehr als 540.000 Bots
 - >2 Milliarden im Internet¹
 - ~ ¼ Online
 - 0,1% in diesem Botnetz
- Wichtiges Teilgebiet
- Wachsender Zweig
- Hand in Hand mit der Host-Forensik

¹Quelle: internetworldstats.com

Fragen?