Visual Malware Analysis

Christian Wojner, CERT.at

Wh01am

Person

- **Christian Wojner**
- **Malware Analysis, Reverse Engineering, Computer Forensics**
- **CERT.at / GovCERT.gv.at**

Publications

- **Papers**
  - Mass Malware Analysis: A DIY Kit
  - **An Analysis of the Skype IMBot Logic and Functionality**
  - **The WOW-Effect**
- **Articles**
  - HITB Online Mag
    - The Art of DLL Injection
    - Automated Malware Analysis - An Introduction to Minibis
  - HAKIN9 Online Mag
    - Minibis
- **Software**
  - Minibis
  - Bytehist (REMnux)
  - Densityscout (REMnux)
  - ProcDOT (REMnux)

Speaker

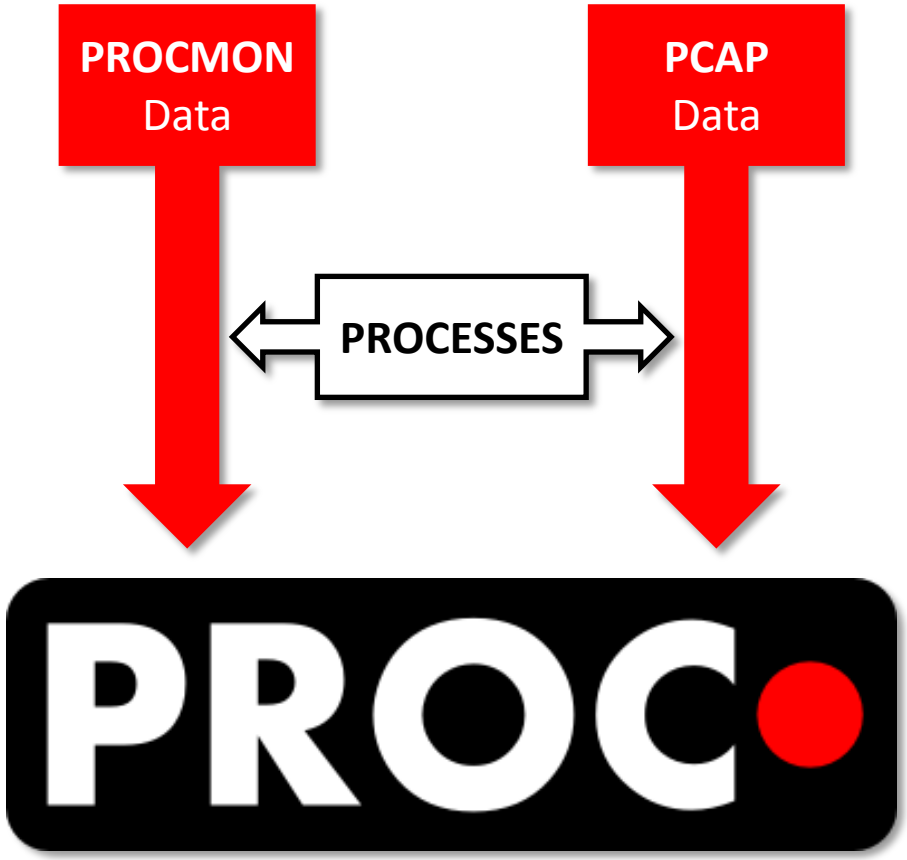
- **FIRST Symposium 2010**
- **CertVerbund-DE 2010**
- **Deepsec 2010**
- **Teliasonera 2011**
- **Joint FIRST/TF-CSIRT Technical Seminar 2012**
- **CanSecWest 2012**
- **CertVerbund-DE 2012**
- **0ct0b3rf3st 2012**
- **SANS Forensic Summit Prague 2012**
- **Deepsec 2012**
- **FIRST Symposium 2013**
- **CertVerbund-DE 2013**
- **0ct0b3rf3st 2013**

Behavioral analysis

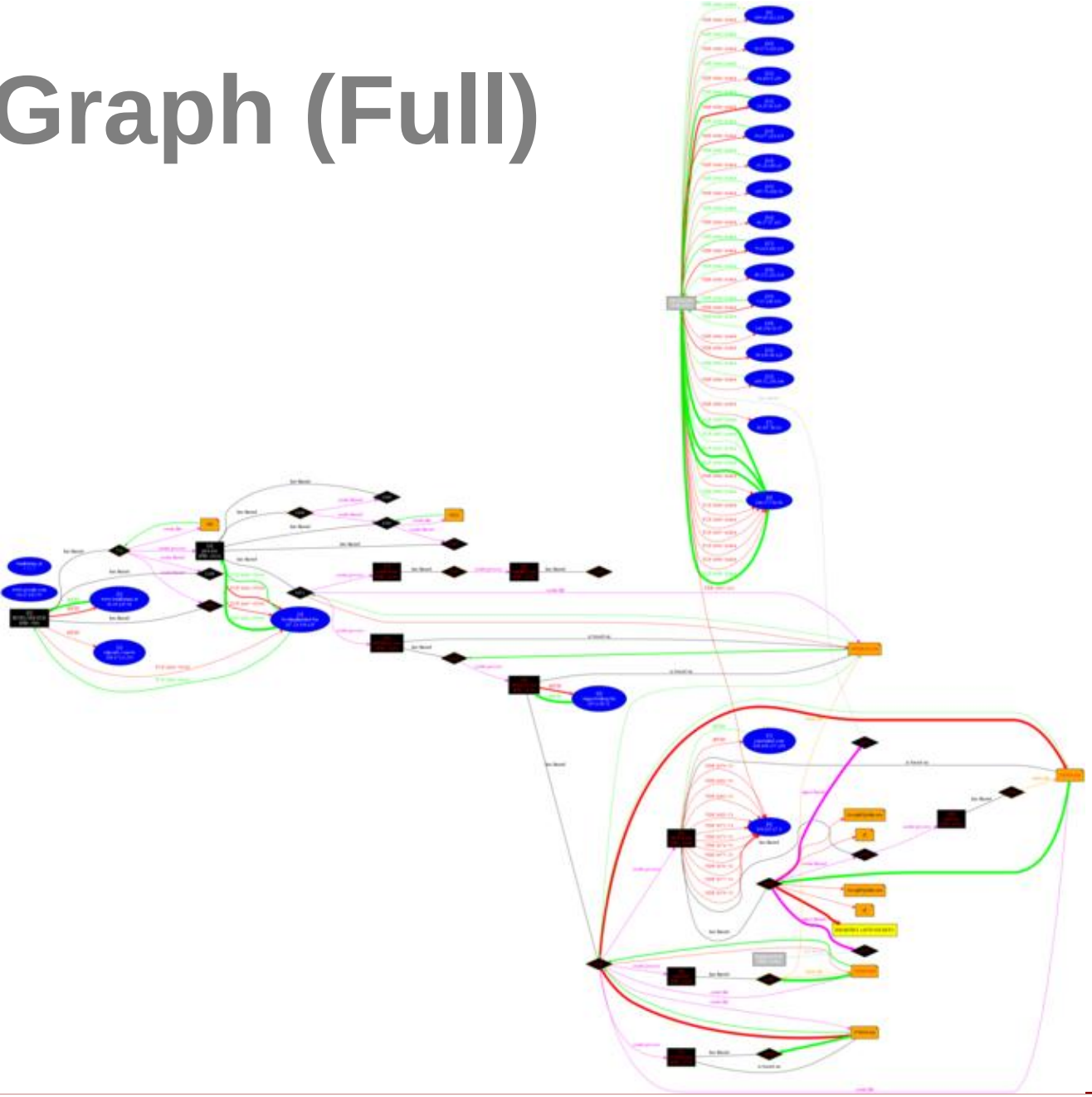
- Monitoring activities

Activity	Procmon	PCAP (Windump, Tcpdump, Wireshark)
Filesystem	✓	✗
Network	✓	✓
Windows Messages	✗	✗
Registry	✓	✗
Process-Management	✓	✗
Thread-Management	✓	✗

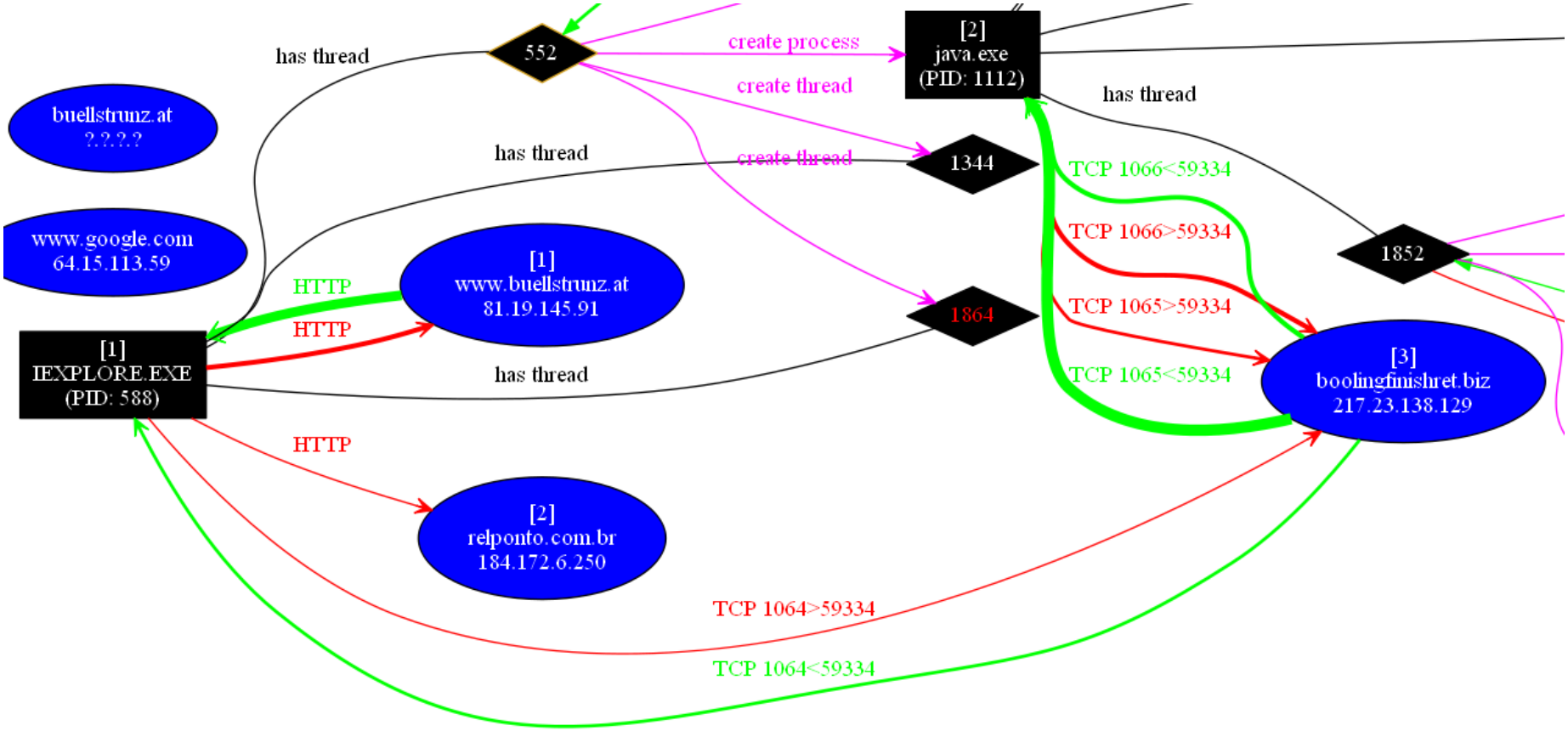
Data-Correlation



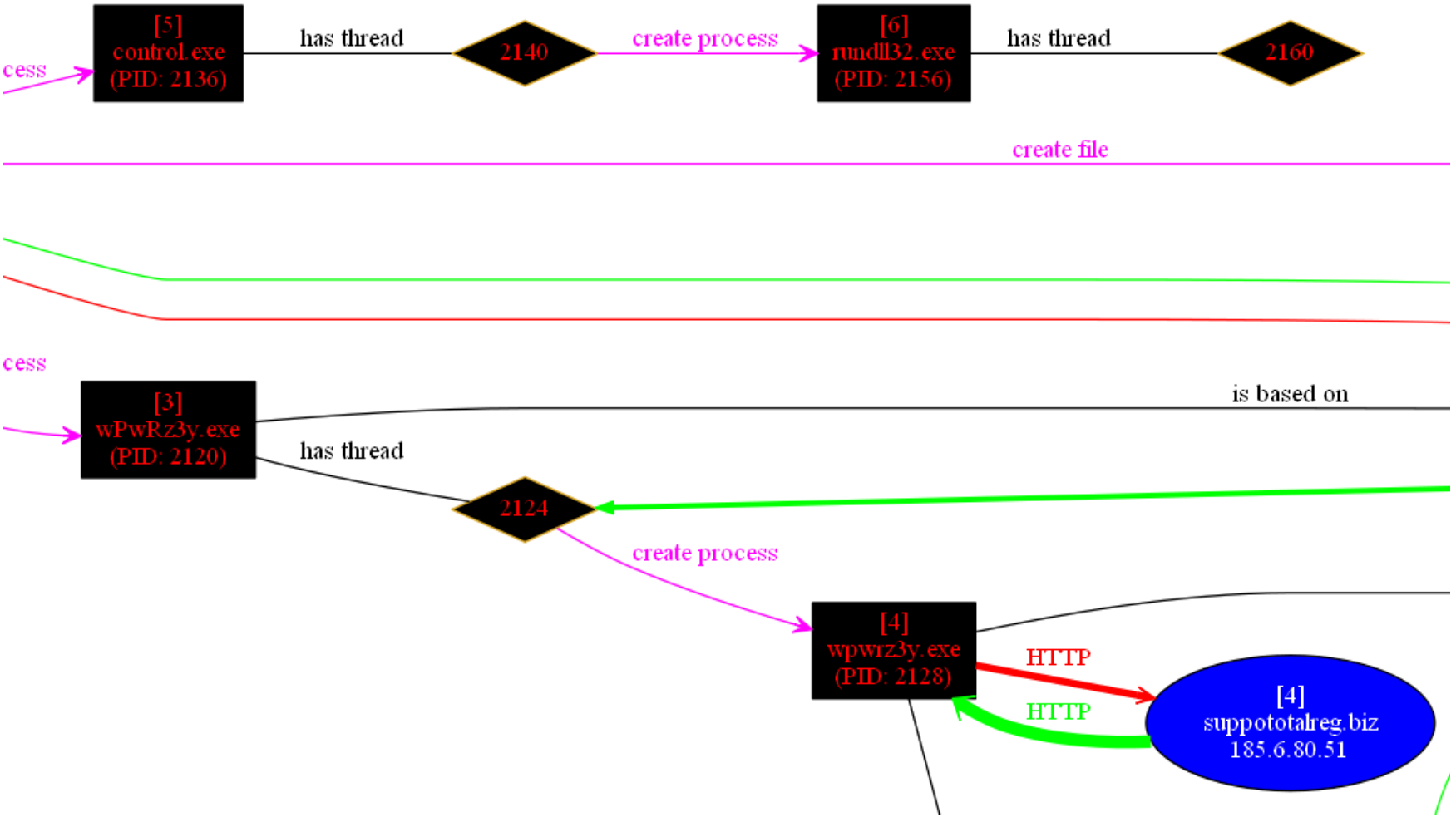
Graph (Full)



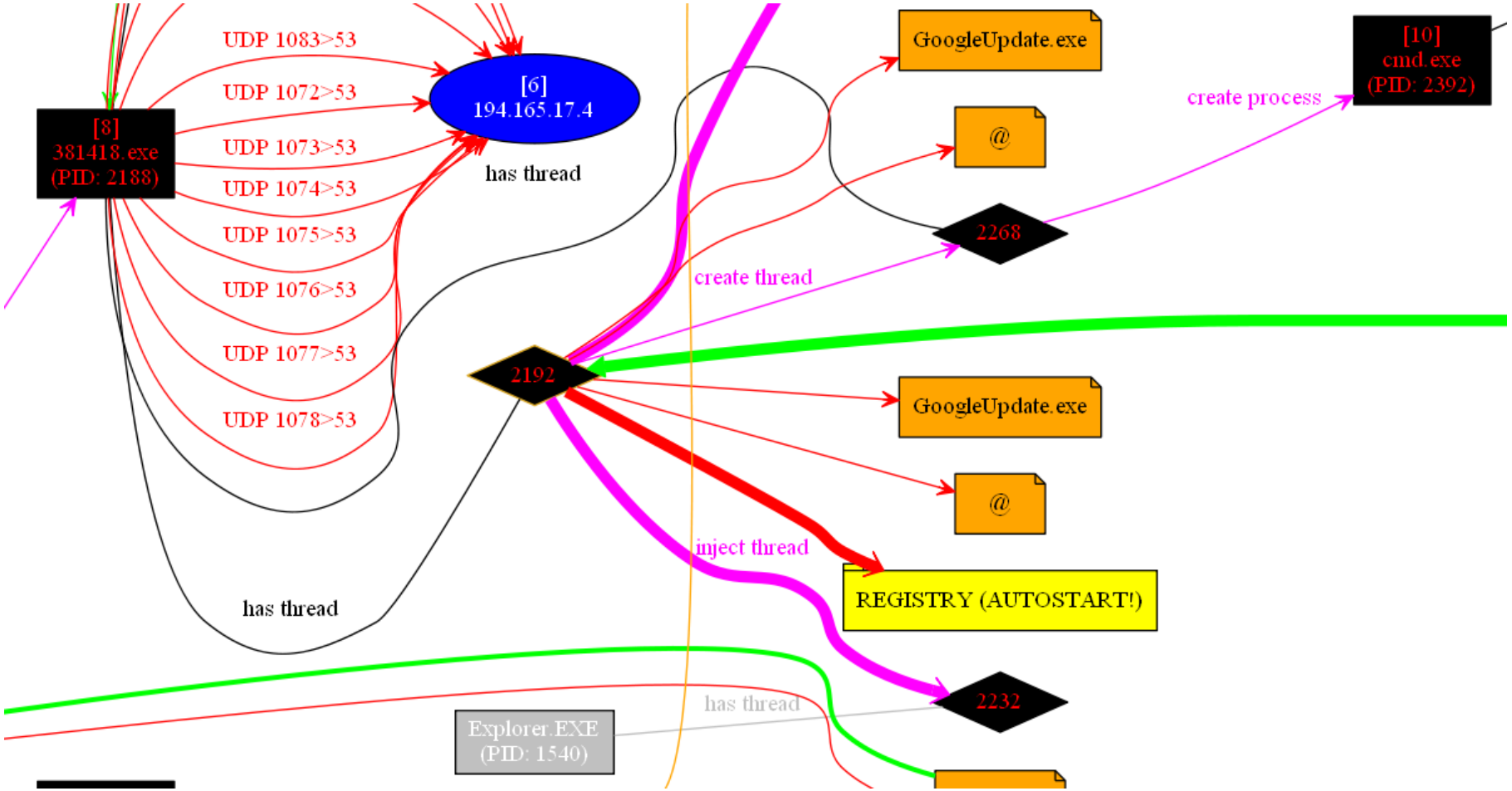
Graph (Part 1/4)



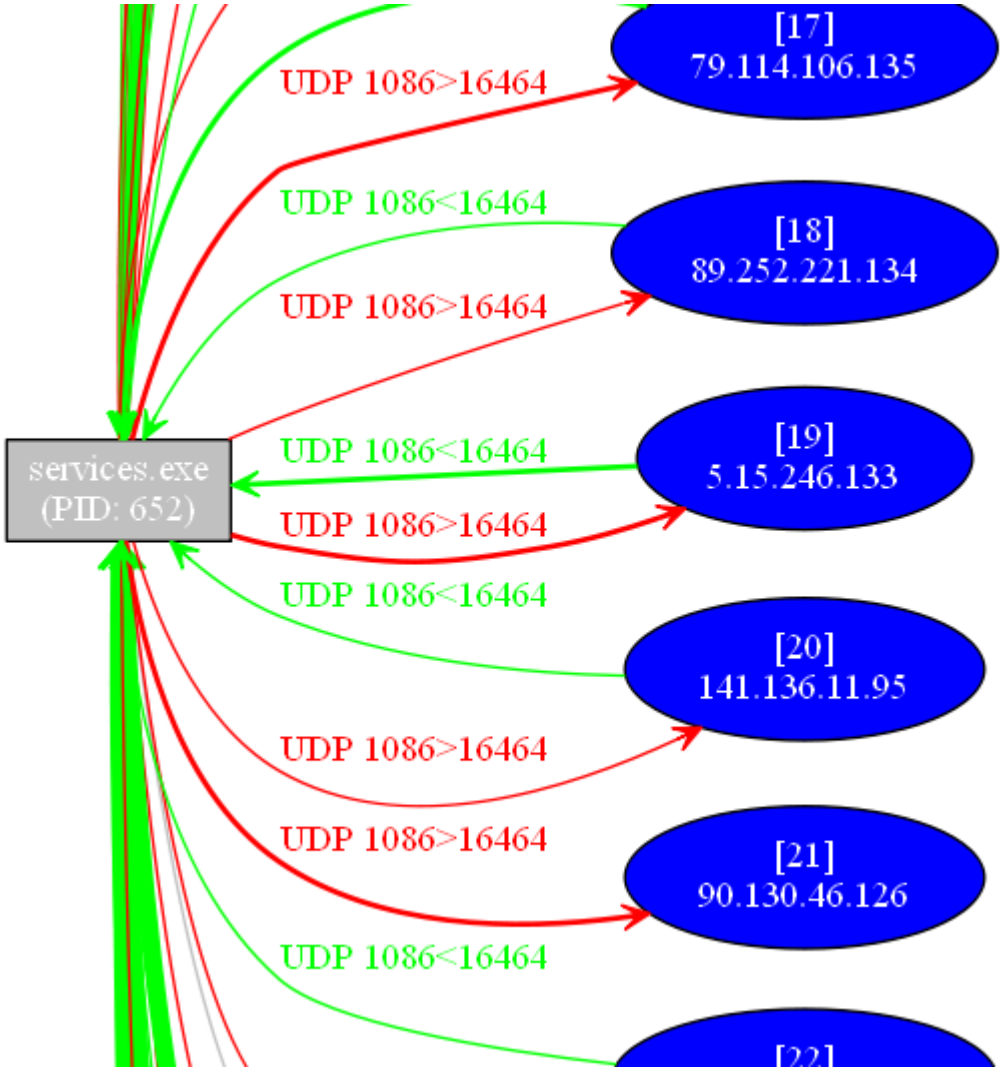
Graph (Part 2/4)



Graph (Part 3/4)



Graph (Part 4/4)



Graph (Animation)

animation.mp4

Roadmap

- Bitmap Exporter
- Plugin Engine
- Frame/Realtime-Relations (statusbar, markers for 1 & 5 sec)
- UTF-8 aware
- Session based filters (+ global ones)
- Filter Manager

- PCAP Integration ++
  - Flow-DB
  - Node/Edge related functionalities
  - Node/Edge related "Open in Wireshark"
- Frame Ranges
- Notes & Tags
- Reporting Module

(Community) Plugins like

WHOIS

PDNS

etc.

- Themes
- Native Rendering

- Support native Procmon log format (RE of .pml)

Get in touch ...

- **Website:**
  - http://www.cert.at/downloads/software/procdot_en.html
- **News:**
  - https://twitter.com/ProcDOT
- **Community:**
  - https://groups.google.com/forum/#!forum/procdot
- **Donate:**
  - http://cert.at/downloads/software/donate_procdot_en.html
- **Contact:**
  - team@cert.at