AMRES
Serbian Academic Network

# BELGRADE SECURITY WORKSHOP 2015

## FORENSIC ANALYSIS

Aleš Padrta

GÉANT

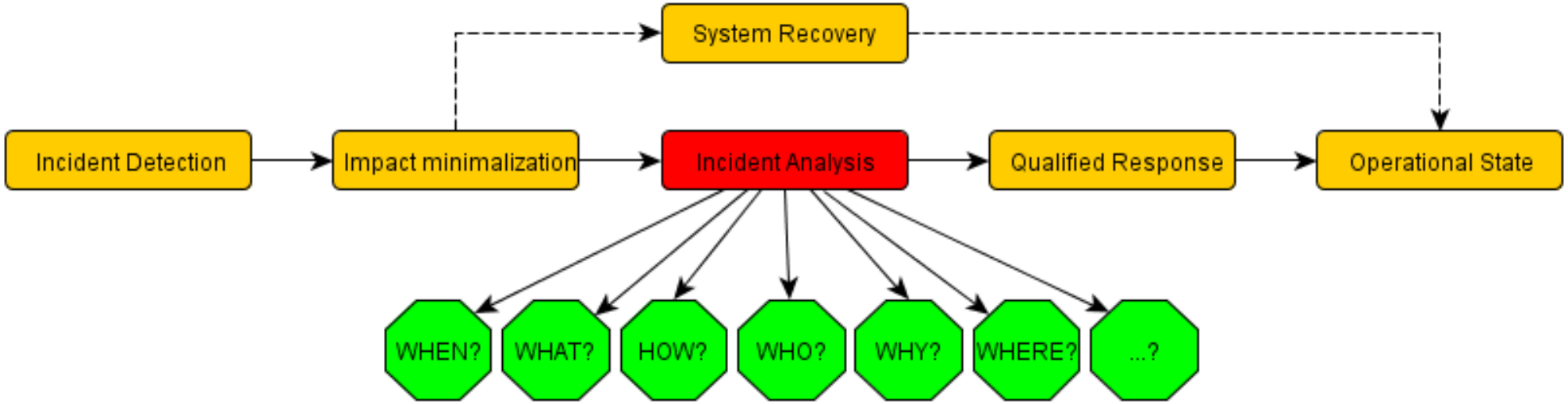
# CESNET, CESNET-CERTS, FLAB

- CESNET – Czech NREN operator
- CESNET-CERTS
  - 2004 – Established
  - 2008 – Accredited CSIRT
- FLAB
  - Forensic LABoratory
  - Established 6/2011
  - Support team for CESNET-CERTS
    - Incident analysis
    - Penetration testing
    - Other services

# Part I. – Brief Introduction

# Why Forensic Analysis?

- Security Incident Handling
  - Standard process



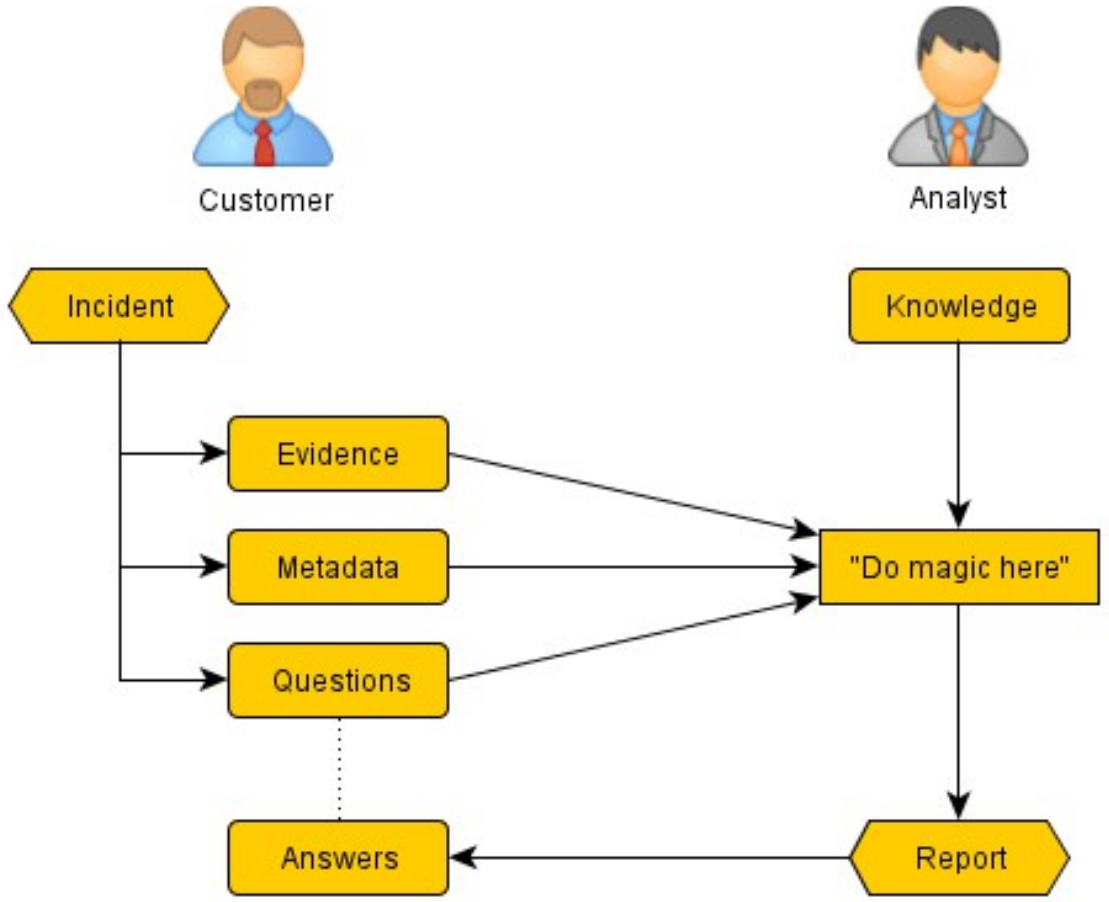

  - Acquiring answers

    ⇨ Detail (forensic) analysis

# Cooperation Scheme

- Customer
  - Problem (Incident)
  - Description
    - Evidence
    - Metadata
  - Questions
- Analyst
  - Own / Outsourced
  - Knowledge

    ⇨ Answers



# Typical Questions

Is some backdoor left there?

When was the server hacked?

Were used antiforesics methods?

When was the system on-line?

Which USB devices were connected?

Which applications were used?

Which webpages were visited?

Which files were modified?

What was the content of communication?

Who used the device?

How to find all infected machines?

What did the user do?

Was some malware present?

Which wifi networks were used?

Which IP addresses were used by attacker?

Which vulnerability has been exploited?

Can you work faster?

# Part II. – Practical Examples

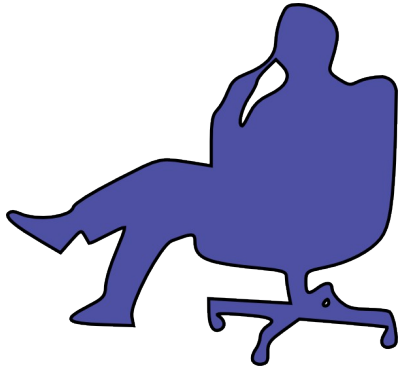
# CASE 1
# Attack Vector on Web server

# Attack vector on Web server

- Metadata
  - Web defacement
  - Suspicious files on HDD
    - Unauthorized application
- Evidence
  - HDD image
- Questions
  - How was the server infiltrated?
  - Which files were created / modified?
  - Did attacker created some backdoor?

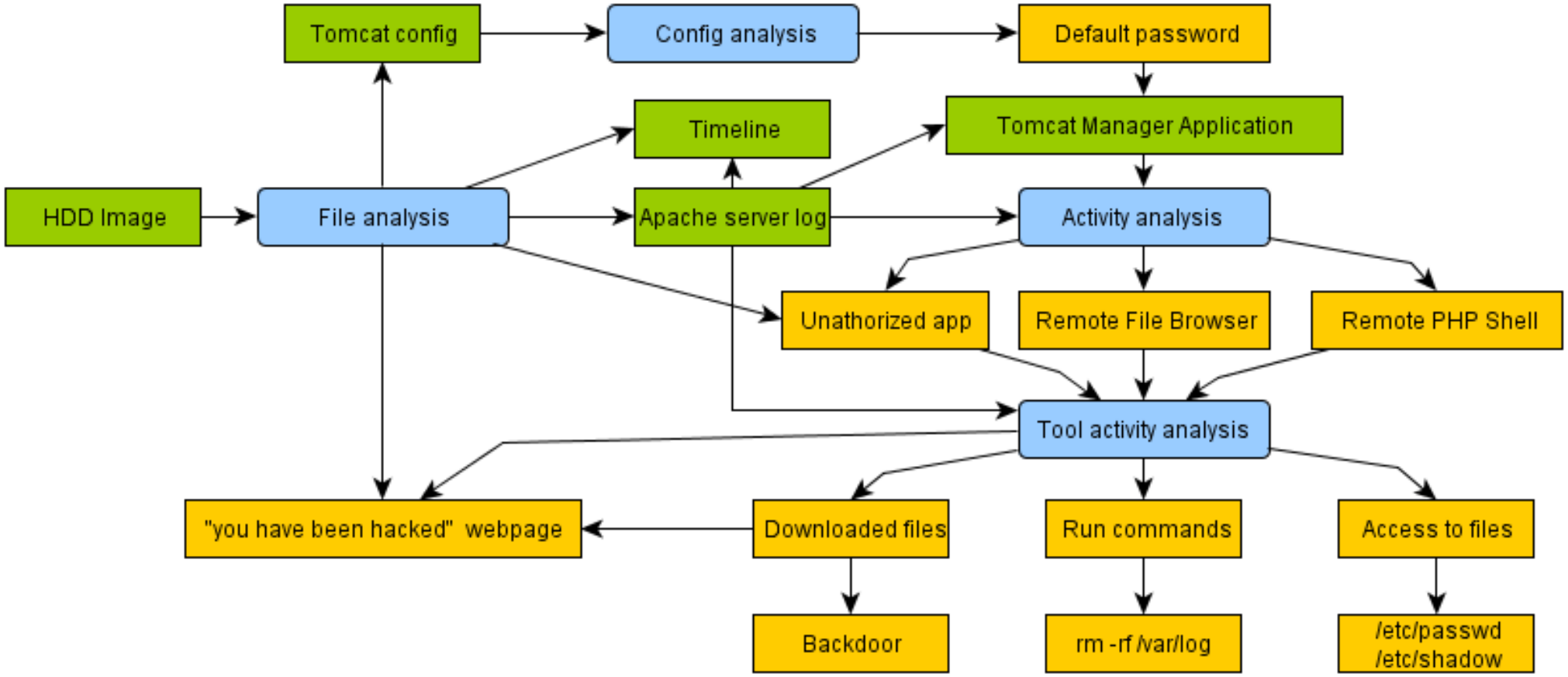
# Attack vector on Web server

- Think Over Phase
  - What we have
    - Files … MAC times
    - Deleted files (Delete = MFT change, data stay on disk)
    - Time information
      - Hack time („you have been hacked“ picture)
      - Last reinstallation time,  shutdown time, admin access, ...
    - Unauthorized application
      - How and when was installed
  - What we can do
    - Create timeline ⇨ activity ⇨ find attacker tools
    - File analysis



# Attack vector on Web server

- Analysis scheme



# Attack vector on Web server

- Event timeline reconstruction
  - T=0 Recon manager/.../howto.html
  - T=+10:09 Passwd guessing (3 times)
  - T=+14:24 Login to manager
  - T=+14:30 Upload „unauthorized app“
  - T=+14:43 Start using „unauthorized app“ (remote shell)
    - Download more tools
    - Download & distribute „you have been hacked“ webpage
    - Access to files
  - T=+20:15 Attempt to antiforensics

# Attack vector on Web server

- Answers to questions
  - How was the server infiltrated?
    - Default + weak password for admin users
  - Which files were created / modified?
    - Acquired list of files
  - Did attacker created some backdoor?
    - Downloaded
    - Tried to install
    - Unsuccessfully

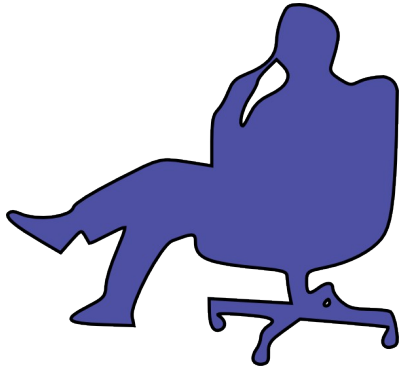
# CASE 2
# Device User Identification

# Device User Identification

- Metadata
  - We found the device
  - Want to handle it properly
- Evidence
  - Nokia N810 + accessories
- Questions
  - Who used the device?
  - When was the device used for the last time?
  - What kind of data was on the device?

# Device User Identification

- Think Over Phase
  - What we have
    - Mobile device
    - Maemo Linux (modified Debian)
      - System partition
      - Data partition
    - Files … MAC times, deleted files
    - Communication device – links to external sources?
  - What we can do
    - Get the system logs ⇨ timestamps
    - Get user data ⇨ timestamps, metadata, contents



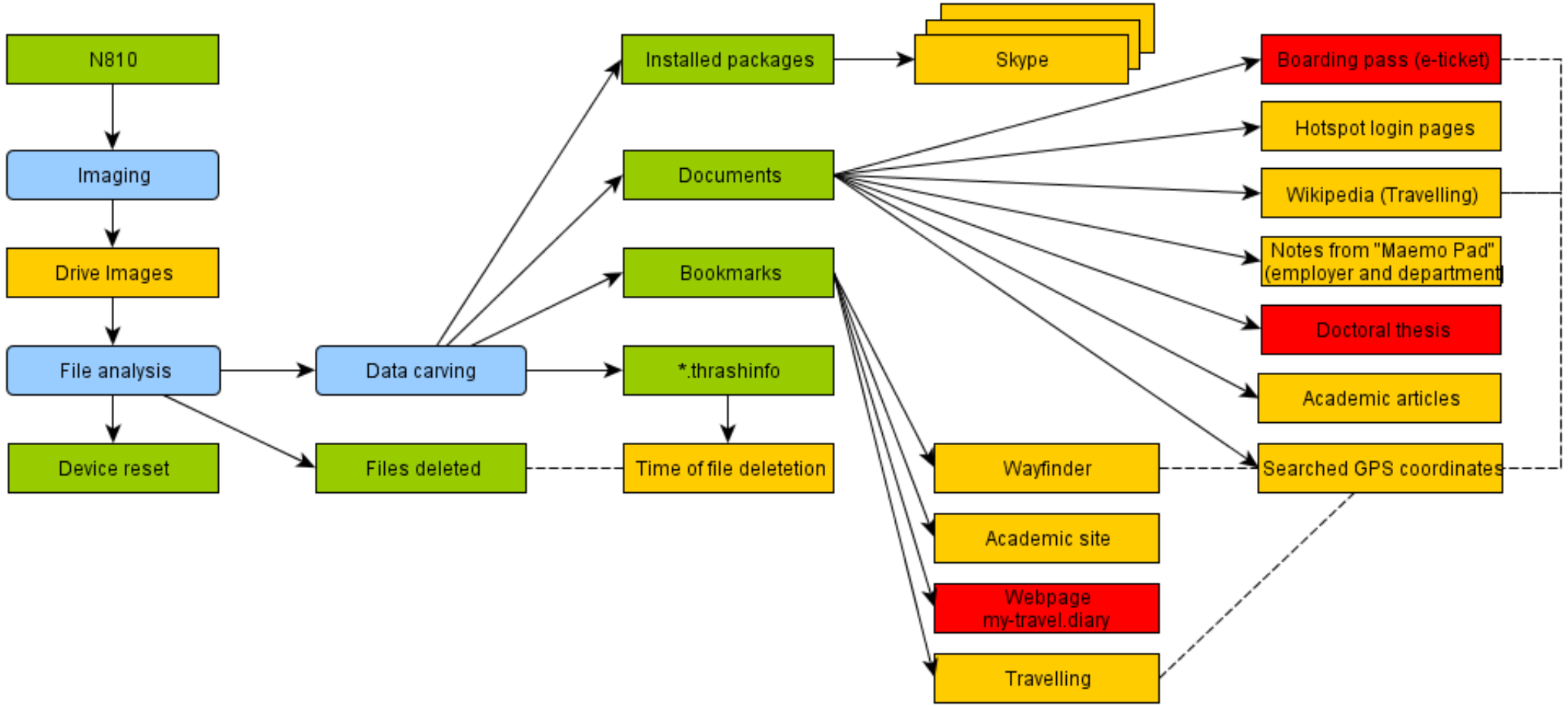
# Device User Identification

- Creating images
  - MicroSD card
    - Connect to PC + FTK Imager
  - Internal memory
    - Application rootsh, DropBear SSH client nad Server

      ⇨ changes to system drive
    - dd, transfer via SSH
  - 3 drives
    - Internal: system (JFFS2), data (FAT32)
    - Removable: microSD card (FAT32)
- Analysis scheme more extensive

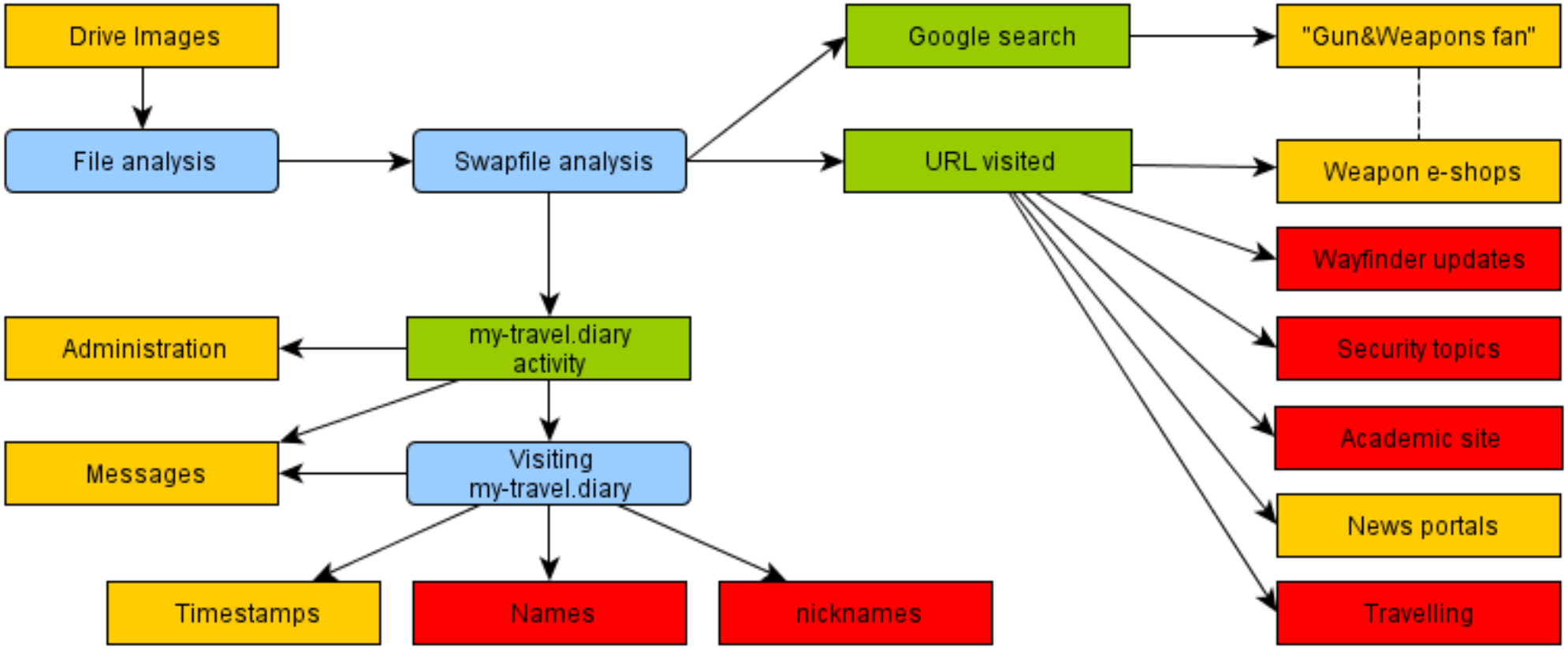
# Device User Identification

- Analysis – Carved files



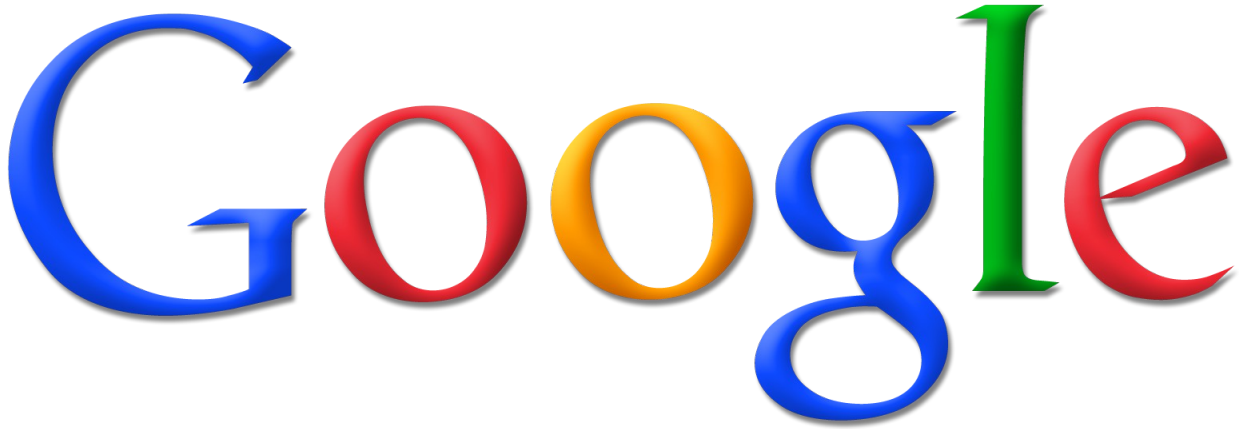
# Device User Identification

- Analysis – Swapfile



# Device User Identification

- Analysis – Data mining
  - Boarding pass
  - Doctoral thesis
  - Web www.my-travel.diary
  - Academic site



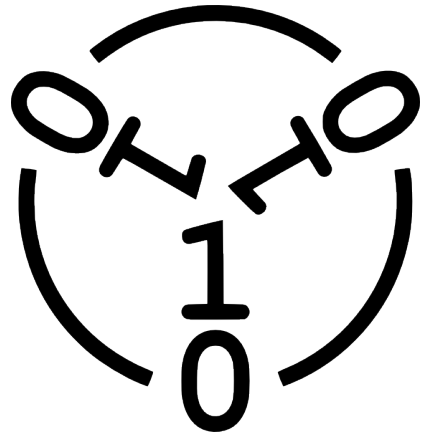
# Device User Identification

- Answers to questions
  - Who used the device?
    - John Excavator (main user)
    - Emily Gold-Digger (secondary user, GF of J.E.)
  - When was the device used for the last time?
    - 20.8.2014 14:13 UCT (data deletion)
  - What kind of data was on the device?
    - Freetime related (travelling, guns hobby)
    - Academic work/study (doctoral thesis, research papers)

# CASE 3
# Quick Malware Analysis

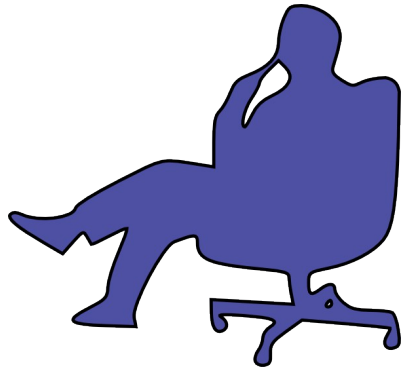
# Quick Malware Analysis

- Metadata
  - Scam e-mails delivered (1000s users)
  - Malware in attachment
  - Without AV detection
- Evidence
  - Several E-mail attachments
- Questions
  - How to identify infected machines?
  - How to stop malware outbreak?
  - How to remove the malware?



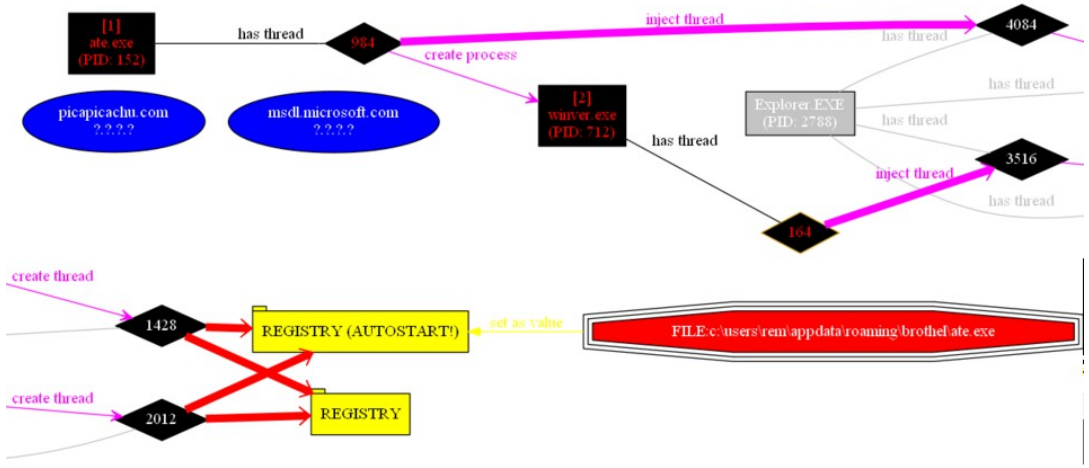
# Quick Malware Analysis

- Think Over Phase
  - What we have
    - E-mail attachments – several malware samples
    - Little time (data for incident response)
    - Typical malware
      - Changes to filesystem (create/modify files)
      - Changes to registry (MS Windows)
      - Communication with dropzone / C&C
  - What we can do
    - Dynamic analysis ⇨ run in monitored environment
    - Analyse changes



# Quick Malware Analysis

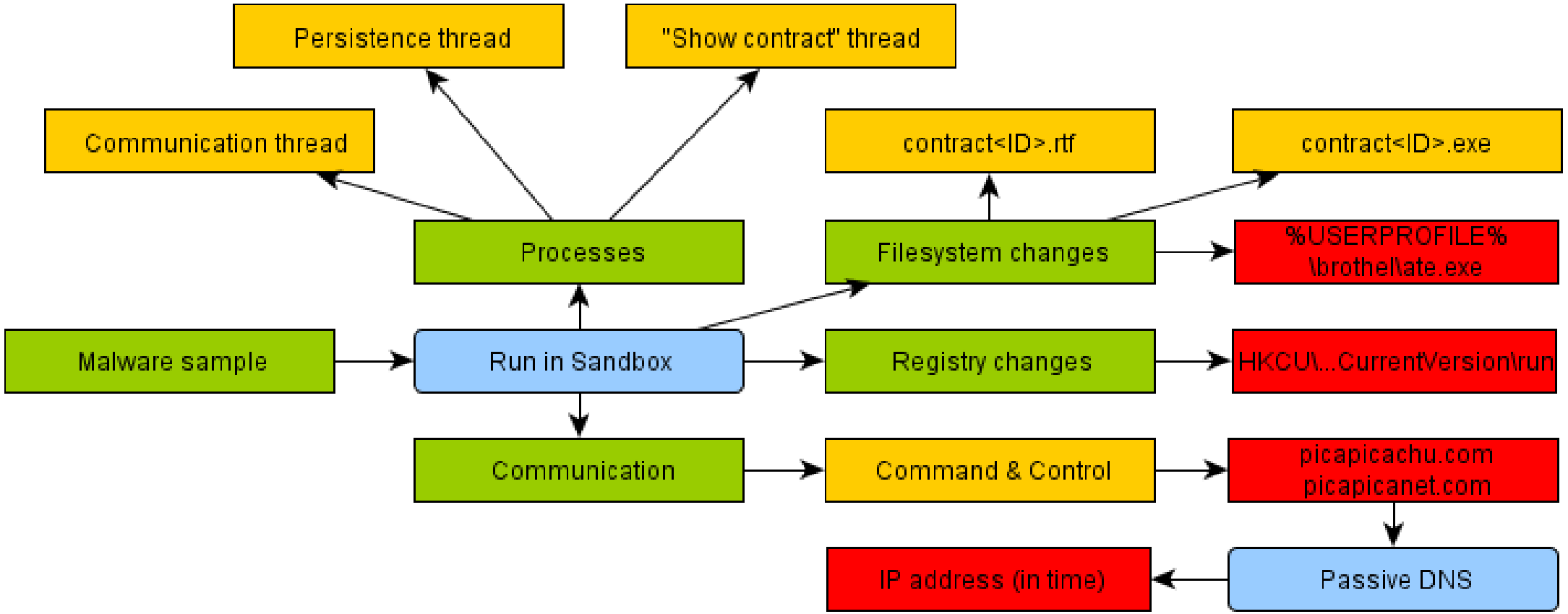
- Controlled environment
  - Virtual machine preparation
    - Process monitor
    - Wireshark
    - CaptureBat
    - RegShot
  - Run malware
    - Collect data
  - Analyse collected data
    - ProcDot (graphic visualization)




Part of ProcDot output

# Quick Malware Analysis

- Analysis results



# Quick Malware Analysis

- Answers to questions
  - How to identify infected machines?
    - Local signs: registry and filesystem changes
    - Network signs: communication with list of IP addresses
  - How to stop malware outbreak?
    - Block creation of „ate.exe“ (manual rule for AV/HIPS)
  - How to remove the malware?
    - Userspace ⇨ clean profile
    - Recommended – reinstall (unknown orders from C&C)

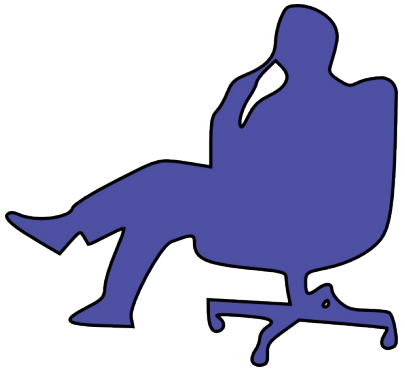
# CASE 4
# Malware Reverse Engineering

# Malware Reverse Engineering

- Metadata
  - Malicious PDF / page visit
  - Locked computers
- Evidence
  - Virtual machines images
  - Memory image
  - Captured communications
- Questions
  - How does the malware infect the machine?
  - Which changes were made on infected machine?
  - Where are the C&C servers?
  - What kind of data is collected and sent to C&C?

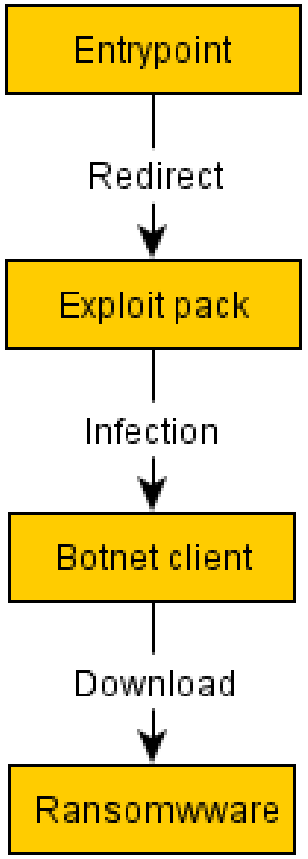
# Malware Reverse Engineering

- Think Over Phase
  - What we have
    - Image of drive & memory
    - Communication
    - Webpages not accessible online
  - What we can do
    - Analyse attack vector
      - Memory, drive, communication
    - Reverse engineering of malware
      - Detail insight
      - IDA Pro, OllyDbg



# Malware Reverse Engineering

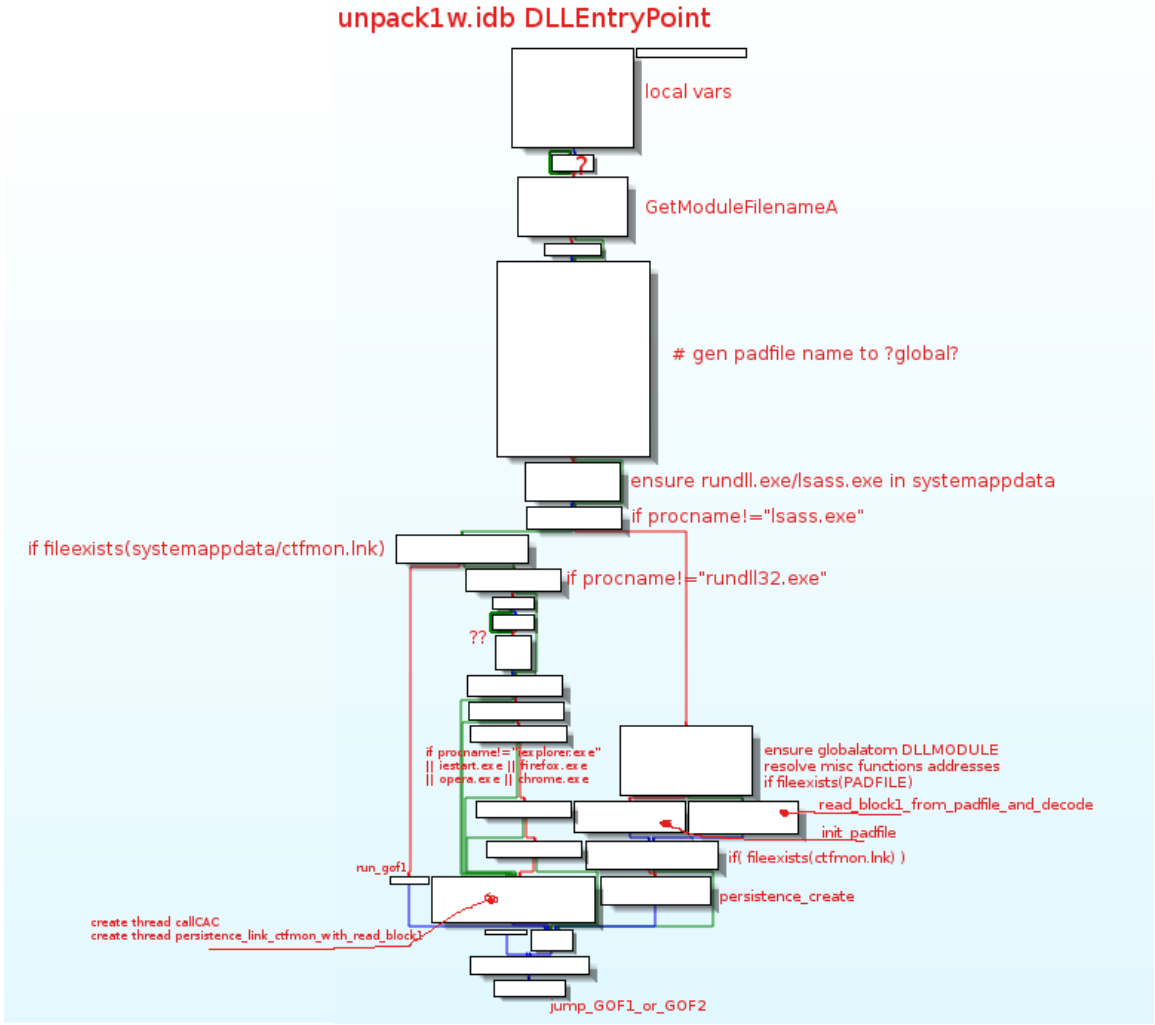
- Attack vector
  - Webpage
    - Entry point
    - Redirect
  - Infect page
    - Professional exploit pack
    - Install botnet client
  - Payload (Ransomware)
    - C&C order
    - Download & Run
  - IP addresses – change in time

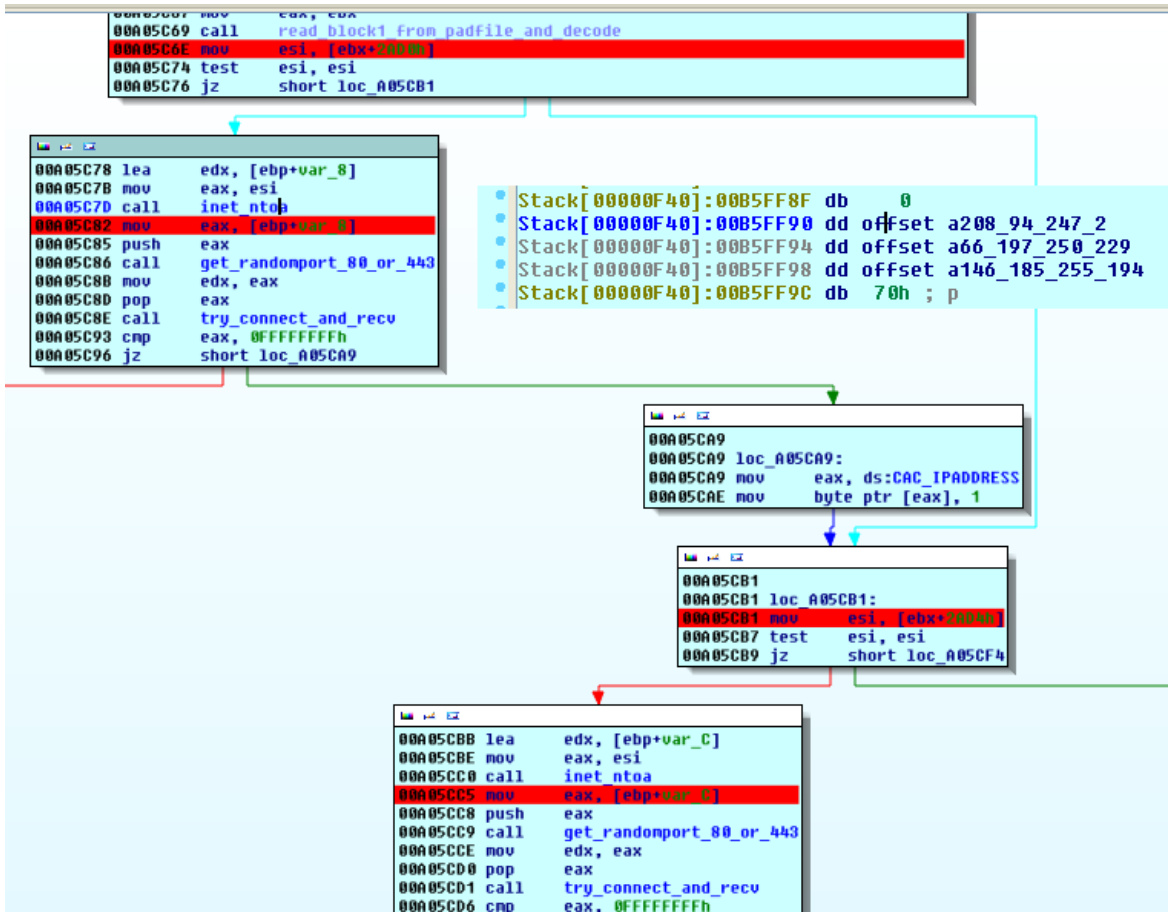


# Malware Reverse Engineering

- Exploit Pack analysis
  - Based on Blackhole
  - Three variants
    - PDF with exploit
    - Font installation
    - Java vulnerability
- Files used by malware (for detail analysis)
  - %userprofile%/Local settings/Temp/wlsidten.dll
  - %allusersprofile%/App Data/netdislw.pad

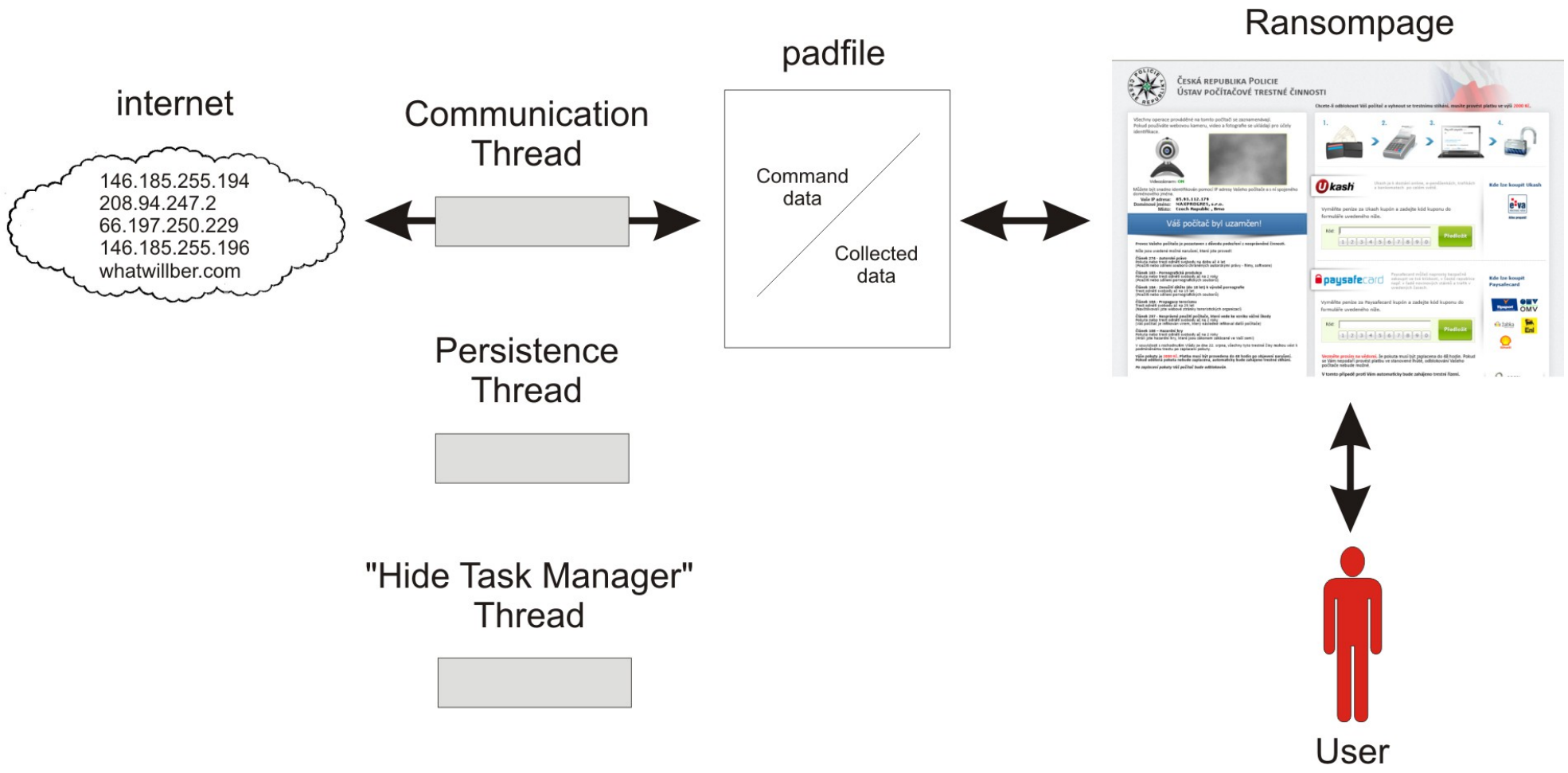
# Malware Reverse Engineering



# Malware Reverse Engineering

- Malware overview



# Malware Reverse Engineering

- How it works
  - Communication thread
    - Code injection to web browser
    - Bypass AV/HIPS rules
  - Persistence thread
    - Write value to registry
    - Each 500ms
  - „Hide Task Manager“ thread
    - Minimize Task Manager window
    - Each 500ms

# Malware Reverse Engineering

- How it works
  - Ransompage
    - Borland Delphi screen
    - StayOnTop
    - Offline code pre-validion
    - Show webcam picture or noise
    - Show IP address geoinfo
  - User profile oriented – can be removed

# Malware Reverse Engineering

- Answers to questions
  - How does the malware infiltrate the machine?
    - One of the exploit PDF/font intallation/java
  - Which changes are made on infected machine?
    - Install botnet client
    - Download and run Ransomware
  - Where are the C&C servers?
    - List of IP addresses + domain name
  - What kind of data is collected and sent to C&C?
    - Volume ID, IP address, webcam picture, entered code

# BELGRADE SECURITY WORKSHOP 2015