

Lightning Talk

Introducing DICOMHawk: A High-Interaction Medical Honeypot

By Georgios Theodoridis, Alexandra Babanuta, Nawras Mouala, **Karina Elzer**, Emmanouil Vasilomanolakis



DICOM Standard/Protocol

Digital Imaging and Communications in Medicine

- International Standard developed in 1980s
- Medical Image Data and Metadata
- Storage and Transmission
 - File Format
 - Communication Protocol

Picture Archiving and Communication System (PACS)

- Medical Imaging System
- DICOM or HL7 Protocol Interfaces
- HTTP Interface



Issues



Outdated Protocol
Lacking Security Features



Exposed Devices
~14.000 Health Devices
and Data Systems*
5.100 DICOM Servers*



No Effective Authorization
Less Than 1%**

*<https://censys.com/blog/state-of-internet-of-healthcare-things>

**https://i.blackhat.com/EU-23/Presentations/EU-23-Yazdanmehr-Millions_of_Patient_Records_at_Risk.pdf

Story Time

“We have become aware of an IP address that appears to be exposing patient data directly to the internet, without authentication”

...

“We've barely dug into the content here, and we see examples of patient names, patient images, and social security numbers that appear to be linked to Danish citizens”

- Detection of DICOM + PACS on the server
- Students DICOMHawk on a Cloud in Norway



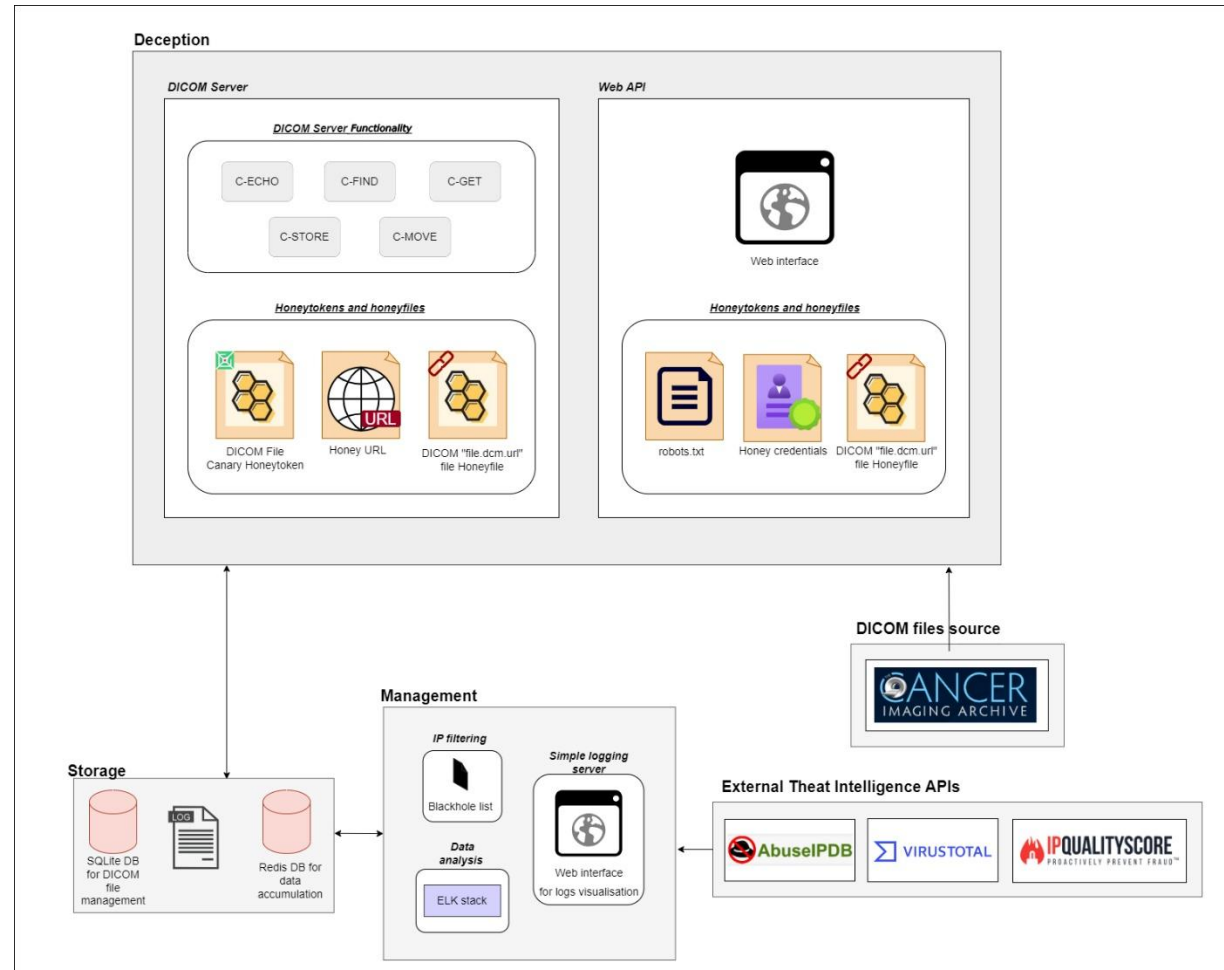
<https://prankshit.com/fake-mail-generator.php>

DICOMHawk Development

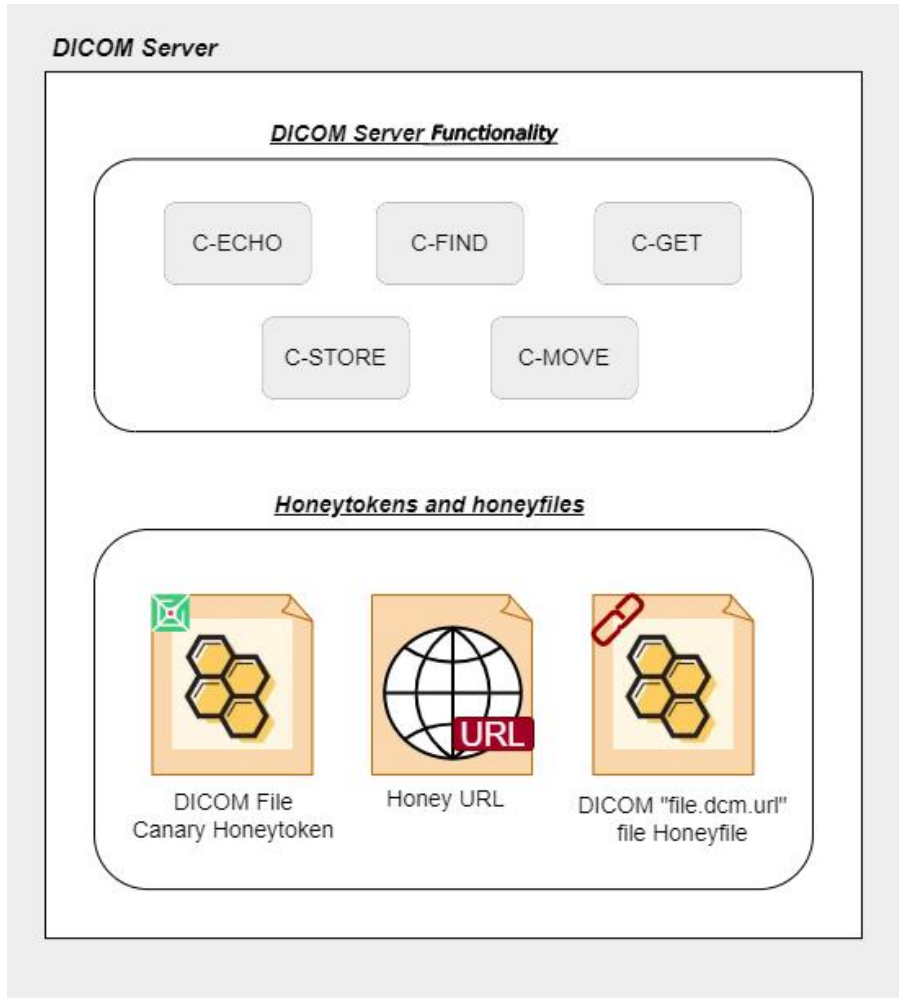
- Github
 - <https://github.com/honeynet/DICOMHawk>
- Creator & Initial Developer:
 - Georgios Theodoridis
- Lead Developers Version 2.0:
 - Alexandra Babanuta
 - Nawras Mouala
- GSoC 2025
 - Anshika Sharma
 - Emmanouil Vasilomanolakis, Karina Elzer, Georgios Theodoridis



Architecture

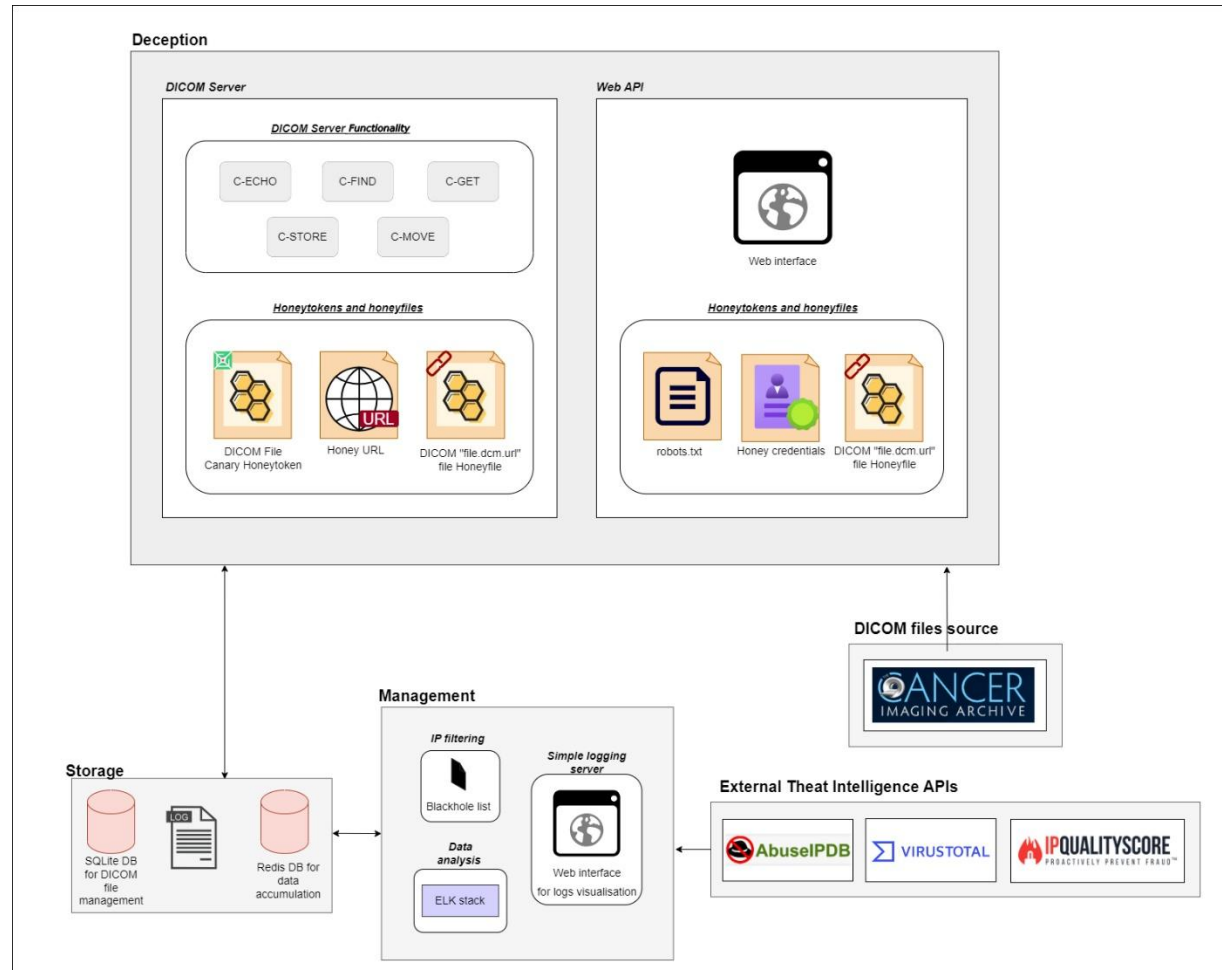


DICOM Server



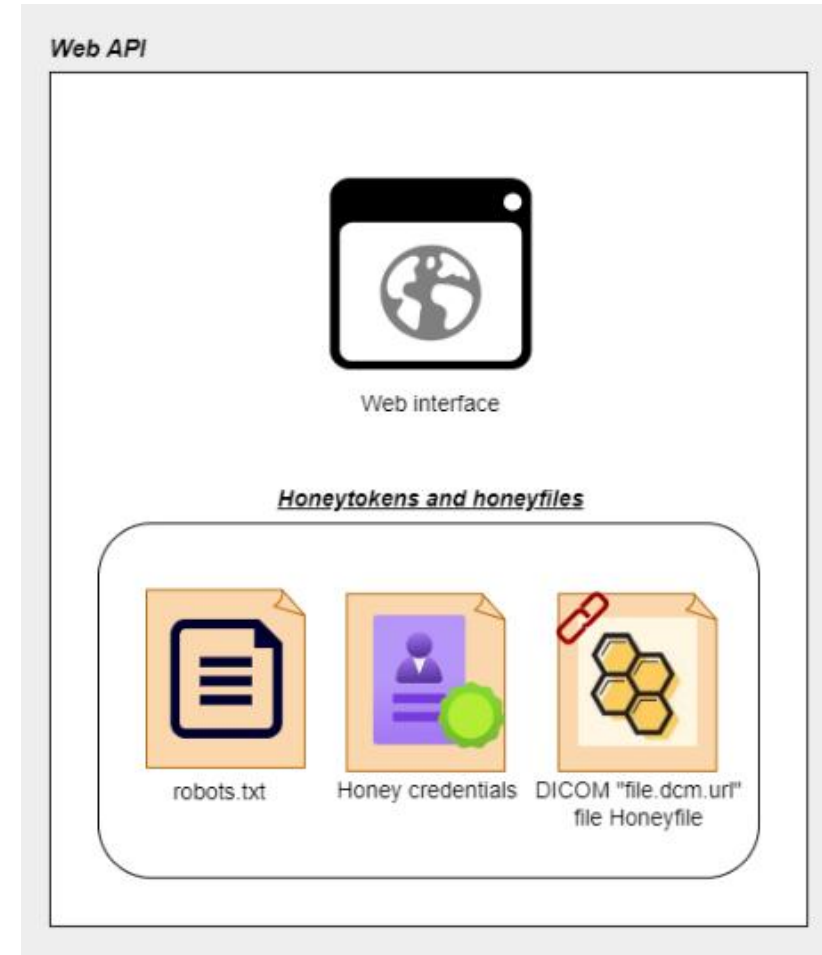
- Functional Basic Operations
 - Error Handling
 - Python Native
 - Real Files with Fake Metadata
 - Dynamic Data/Responses
 - Additional Deception
 - Injected Files
- Realistic Interactions Possible

Architecture



Web API

- Web Interface – PACS
 - Fake Routes
 - Honeycredentials
 - Same Data as DICOMServer
- Not just stand alone DICOM,
Additional Service



Dicompot Comparison

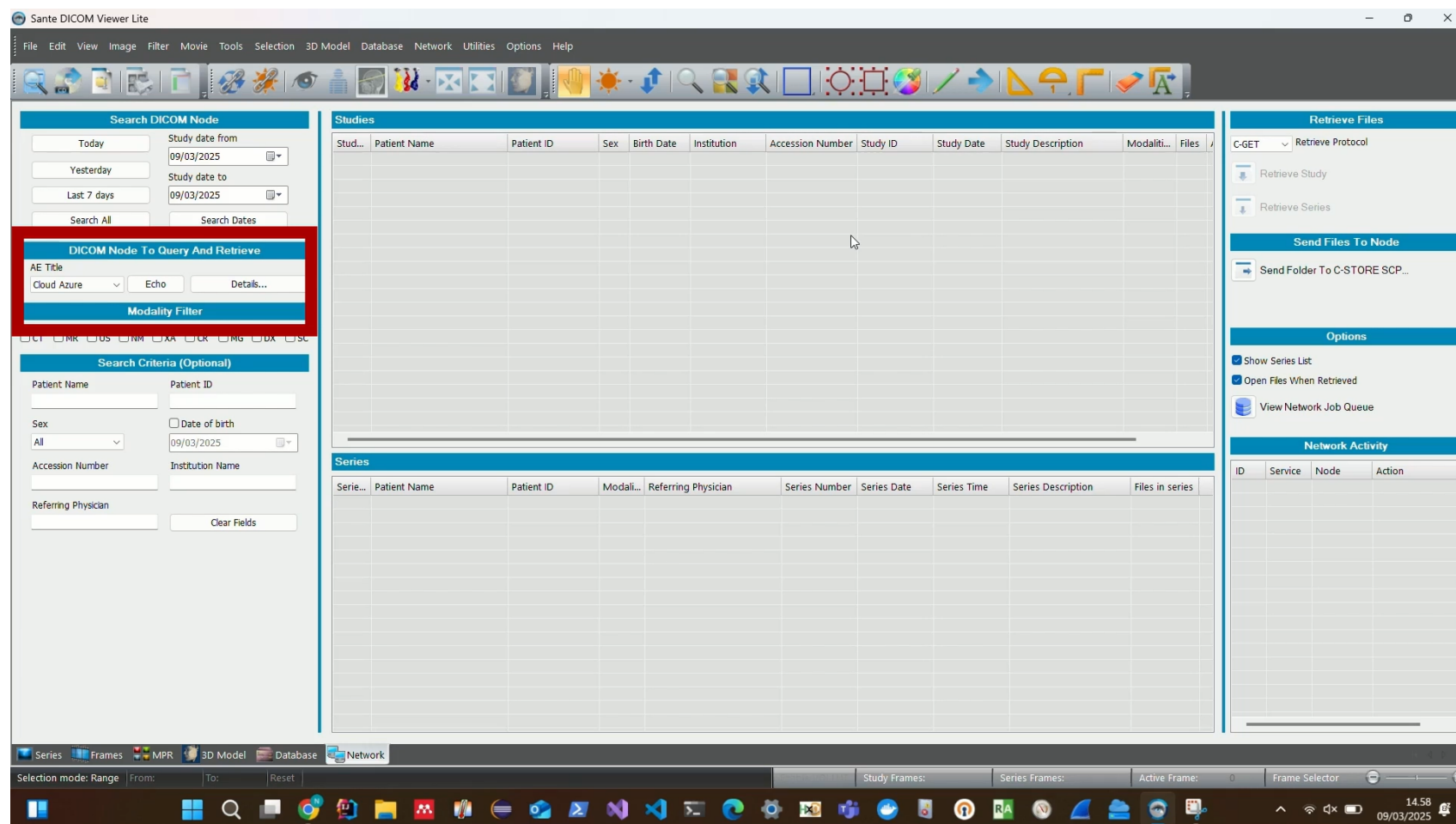
DICOMHawk

- High Interaction
- Additional Service + Deception
- Not Recognized as Honeypot (by Shodan)

Dicompot

- Low/Medium Interaction
- Less Realistic
- Can be Fingerprinted

Demo



Current Results

DICOMHawk

- 01.01.2025 – 15.05.2025
- Open Ports: 104
- Only Scanning, No Interaction

	Unique IPs	Total Seen
<u>All</u>	<u>126</u>	<u>655</u>
Censys	60	163
Shodan	26	408
Internet Measurement	25	48
Onyphe	5	10
Cloud	4	12
Internet Census	3	5
China ISPs	3	9

Current Results

DICOMHawk

- 01.01.2025 – 15.05.2025
- Open Ports: 104
- Only Scanning, No Interaction

Dicompot

- 12.01.2025 – 30.04.2025
- Open Ports: 104 + 11112
- 5 Interactions (Same IP)

	Unique IPs - Hawk	Total Seen - Hawk	Unique IPs - Pot	Total Seen - Pot
<u>All</u>	<u>126</u>	<u>655</u>	<u>648</u>	<u>1789</u>
Censys	60	163	173	243
Shodan	26	408	15	123
Internet Measurement	25	48	-	-
Onyphe	5	10	47	49
Cloud	4	12	101	966
Internet Census	3	5	13	16
China ISPs	3	9	10	11
Palo Alto	-	-	203	260
Other	-	-	86	221



Lightning Talk

Introducing DICOMHawk: A High-Interaction Medical Honeypot

By Georgios Theodoridis, Alexandra Babanuta, Nawras Mouala, **Karina Elzer***, Emmanouil Vasilomanolakis

*kaelz@dtu.dk