Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy

Kevin Conlan MS, Ibrahim Baggili PhD, Frank Breitinger PhD

Graduate Researcher & UNHcFREG Member
Presenting @ DFRWS USA 2016, Seattle

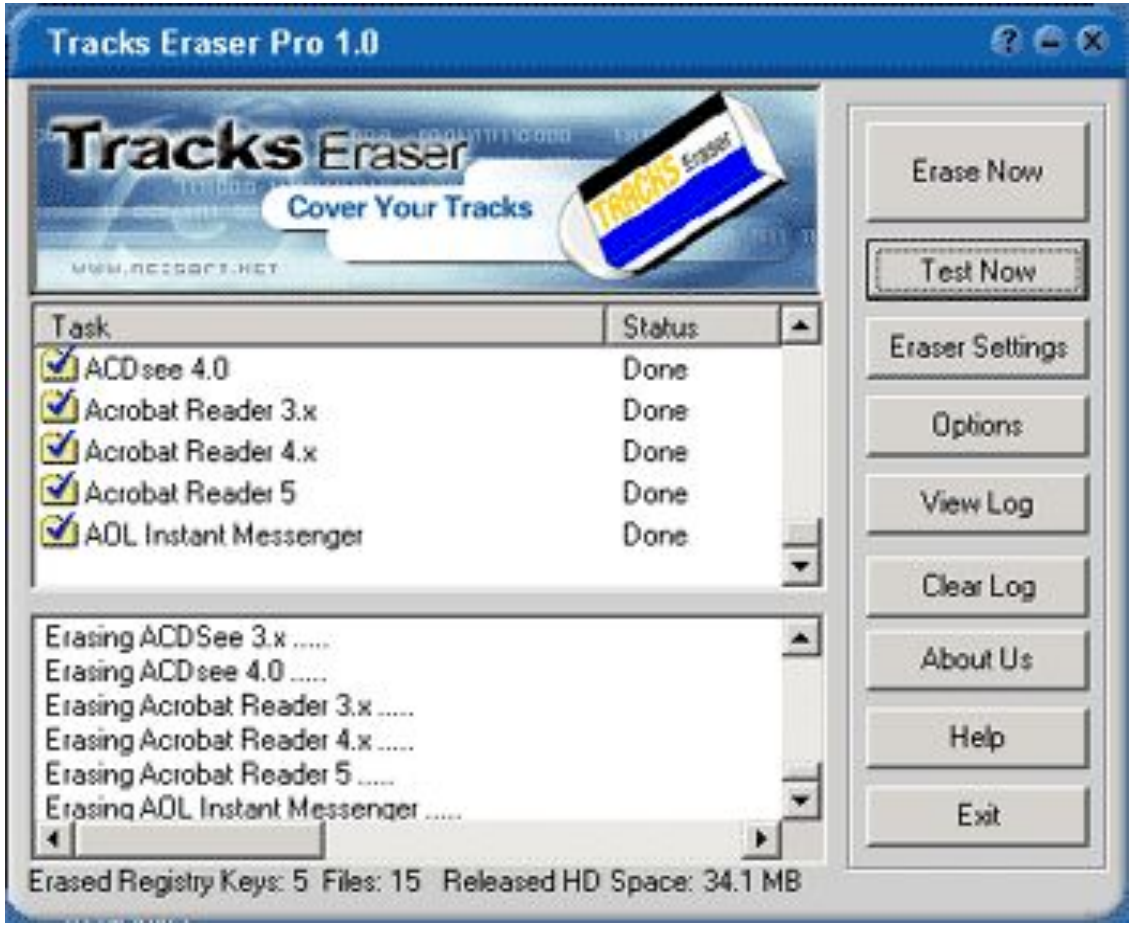
University *of* New Haven
Cyber Forensics Research & Education Group

UNHcFREG

UNHcFREG

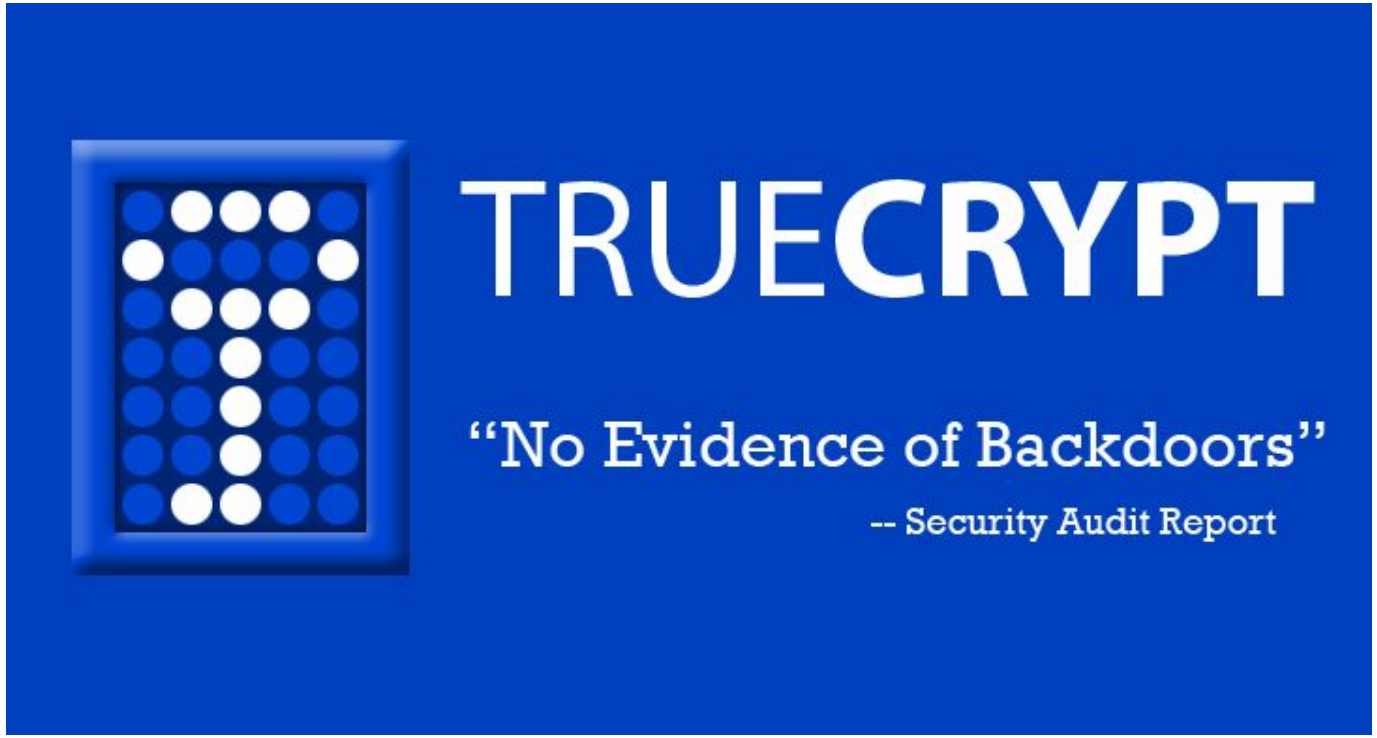
Anti-forensics: Tools and techniques used to invalidate the digital forensic process.

Do you consider *Tracker Eraser Pro* as an anti-forensic tool?



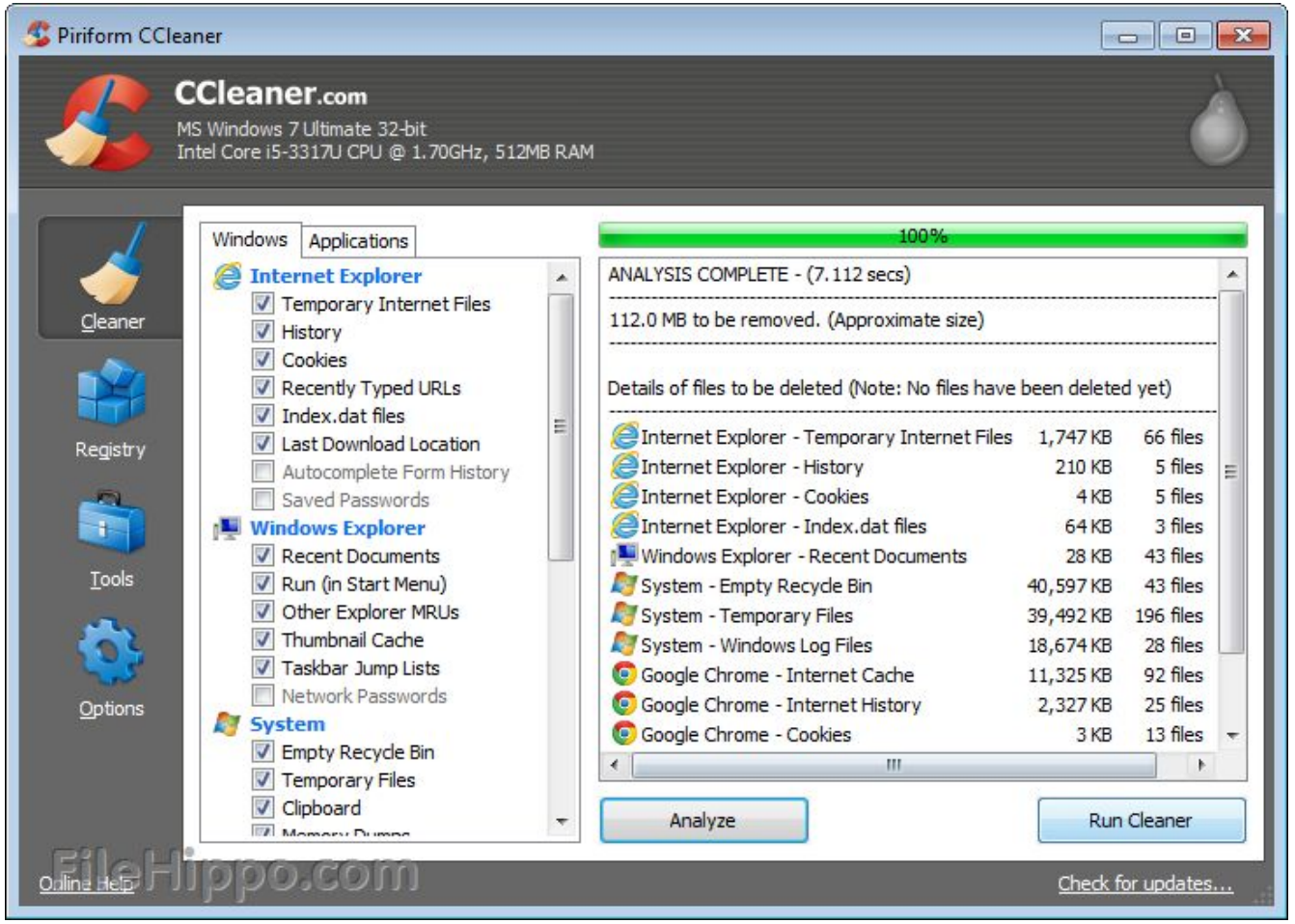
UNHcFREG

How about this encryption tool?



UNHcFREG

And this popular disk cleaner/registry wiper?



And this VPN?

UNHcFREG

Agenda

- Problem statement
- Contribution
- Related work
- Methodology
- Results & discussion
- Limitations
- Conclusions & future work

Problem statement

Not enough research on anti-forensics. Baggili et al. (2012): Out of 500 digital forensic research papers, only 2% pertained to anti-forensics.

Anti-forensic tools and techniques can be used to:

- Remove
- Alter
- Disrupt

Or otherwise interfere with evidence of criminal activities on digital systems.

Contribution

I. A categorical data set of 308 anti-forensic tools.

II. An extended version of the Rogers (2006) anti-forensic taxonomy (Figure 1).

III. The calculated hash values of 2780 unique installation-related files of the anti-forensic tools, and an analysis of their presence in the newest 2016 NSRL[1].

[1] http://www.nrsrl.nist.gov/(last accessed 2016-02-10).

Figure 1:

- **Data hiding**
  - Encryption
  - Steganography
  - Other forms of data hiding
- **Artifact Wiping**
  - Disk cleaning utilities
  - File wiping
  - Disk degaussing / destruction techniques
- **Trail obfuscation**
- **Attacks against computer forensic tools and processes**

Related Work

Harris (2006): There are no general or contemporary frameworks with which to analyze anti-forensics. There a few general groupings of anti-forensic methods, but no identifiable groupings of anti-forensic software.

Garfinkel (2007): Tools that can evade forensic processes are widely available.

Geiger (2005): Entire software packages exist that are designed for anti-forensics.

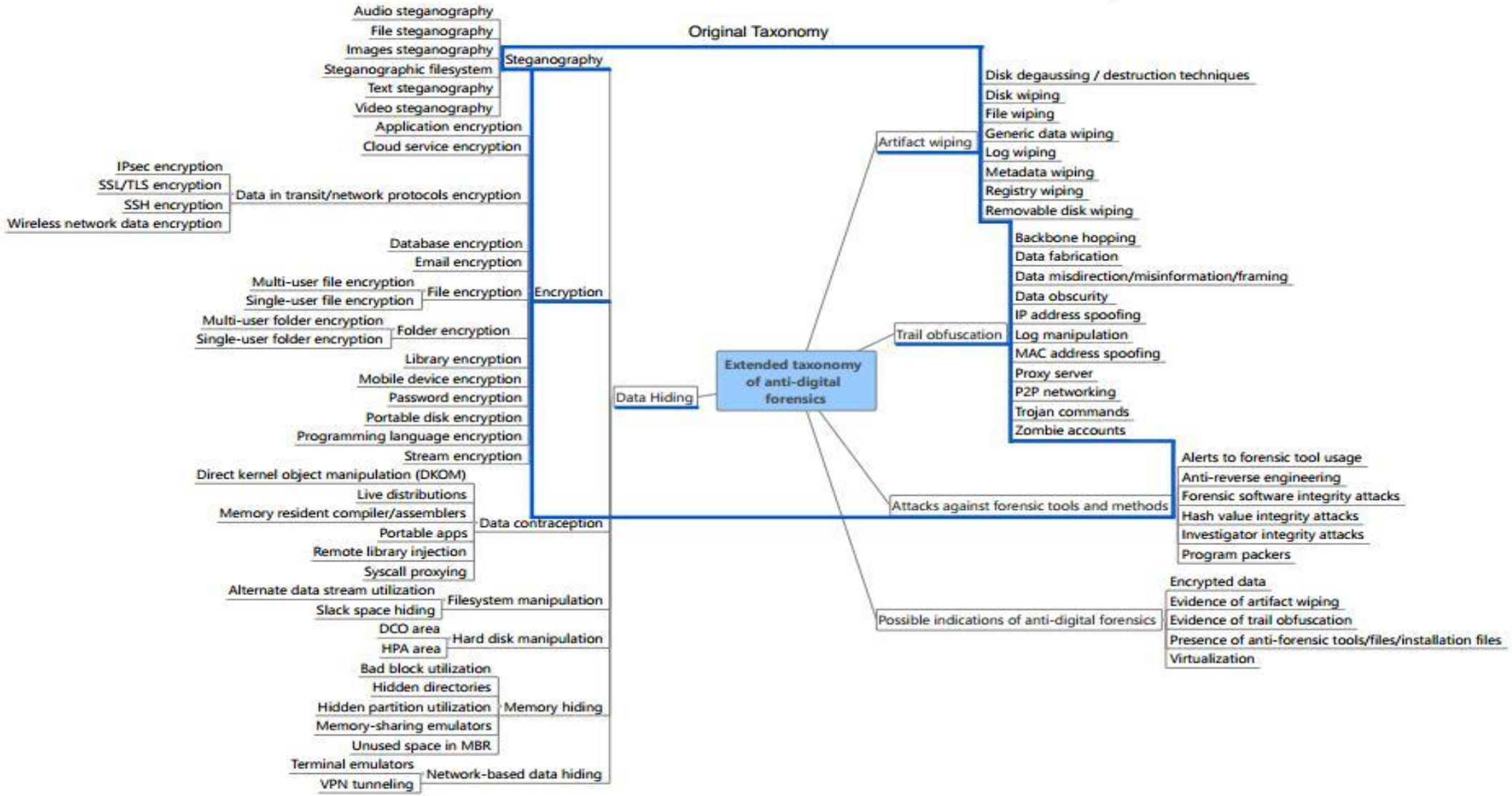
Methodology

Our methodology included the following overarching steps:

I. **Data set creation**
II. **Data set organization**
III. **Data set analysis**
IV. **Hashing**
V. **Data set comparison with NSRL**
VI. **Extended taxonomy creation**

Figure 2: Extended Taxonomy of anti-forensics

* Items underlined and inside the blue frame were categories previously identified in the original anti-forensics taxonomy proposed by Rogers (2006). Our taxonomy is an extended, more granular version of the old one.



Results and discussion

Comparing anti-forensic tools hashes to the NSRL

Python script was written to acquire 2780 unique MD5 and SHA1 hash values of the anti-forensic tool installation related files, and was compared against the newest 2016 Reference Data Set (RDS). Only 423 hashes were found.

The unmatched hashes would be example *Presence of anti-forensic tools/files/installation files* under the category of *Possible indicators of anti-digital forensics.*

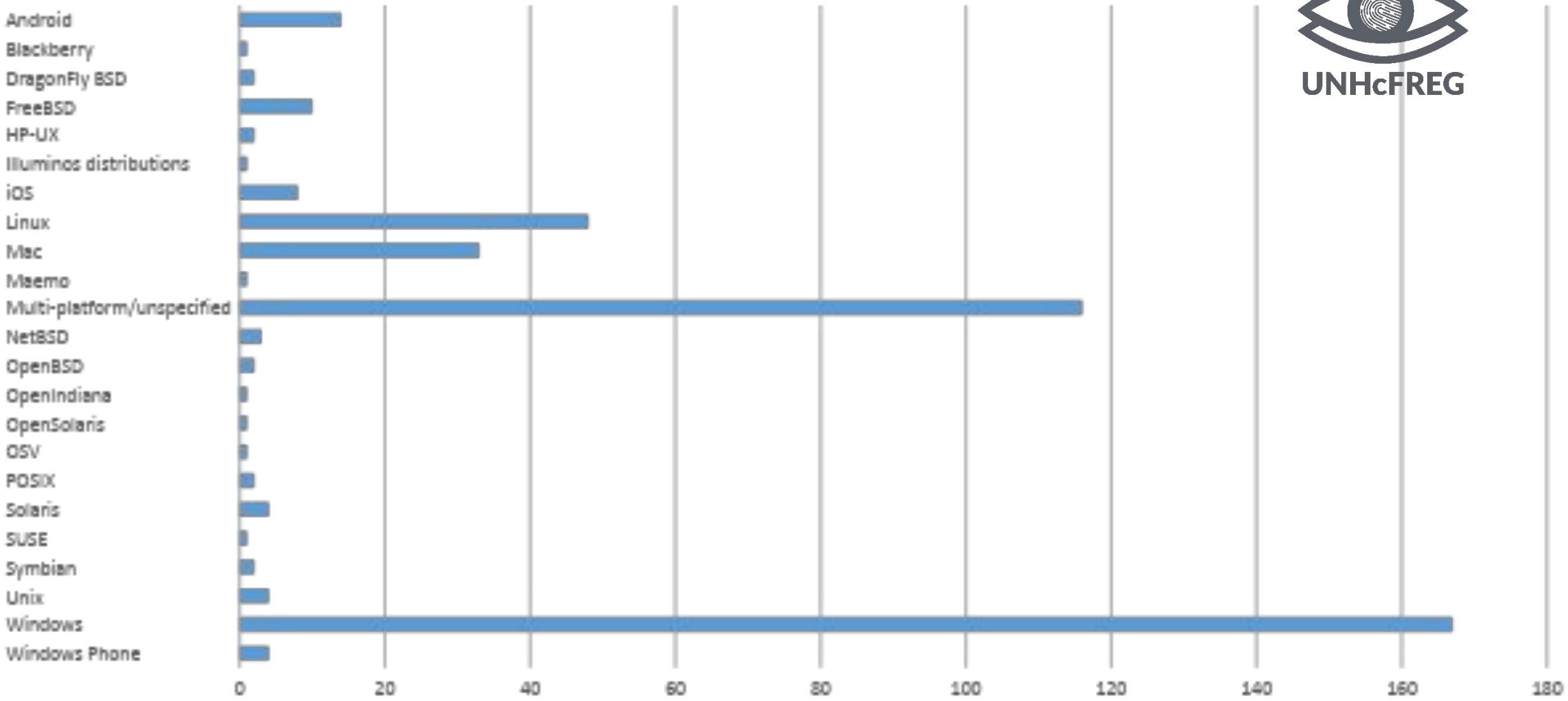
Figure 3: Number of tools found per anti-forensic category

Data hiding (153)
–Encryption (127)
—Disk (46)
—Email (9)
—File (19)
—Filesystem (9)
—Data-in-transit / network protocol (14)
—Password (7)
—Mobile device (8)
—Portable drive (5)
—Application (2)
—Cloud service (3)
—Programming language (2)
—Library (3)
–Steganography (16)
—Image (4)
—Text (9)
—Filesystem (3)
–Data contraception (1)
—Syscall proxying (1)
–Filesystem manipulation (2)
—Slack-space hiding (2)
–Memory hiding (1)
—Memory-sharing emulators (1)
–Network-based data hiding (6)
—Terminal emulators (3)
—VPN tunneling (3)

–Artifact wiping (113)
—File wiping (27)
—Disk wiping (28)
—Removable disk wiping (3)
—Generic data wiping (23)
—Registry wiping (29)
—Disk degaussing / destruction techniques (2)
—Metadata wiping (1)
–Trail obfuscation (38)
—P2P networking (33)
—IP address spoofing (1)
—Data fabrication (2)
—Data misdirection / misinformation (1)
—Proxy server (1)
–Attacks against forensic tools & processes (4)
—Program packers (4)

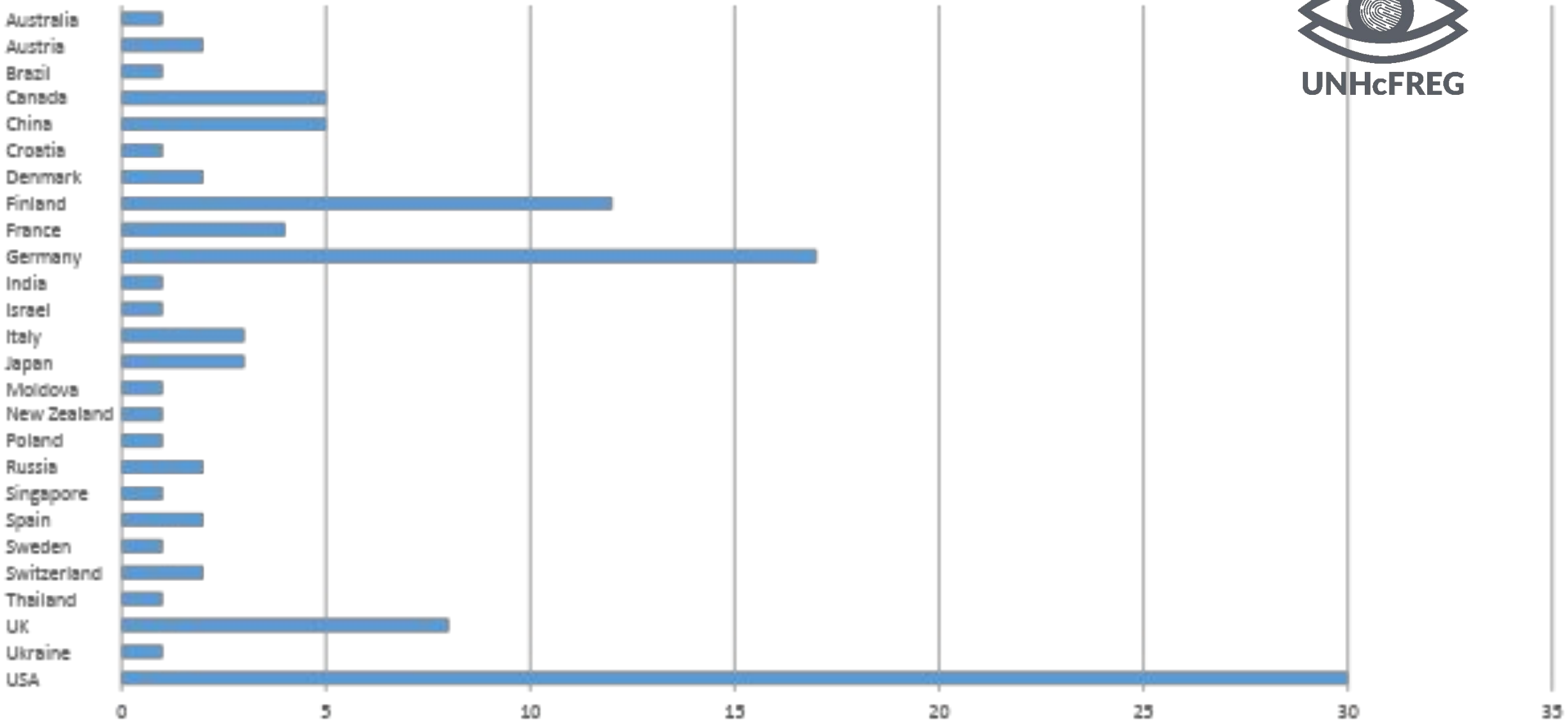
UNHcFREG

Figure 4: Instances of operating systems/platforms



UNHcFREG

Figure 5: Tools by identifiable country of origin



Limitations

A considerable limitation was the number of software tools that may be considered “anti-forensic” in nature is vast and continuously growing.

It is difficult to determine the entire scope of the anti-forensics domain. However, this is not as much a “limitation” as it is an opportunity for future research endeavors.

Conclusions and future work

The goals of this work was the following:

A categorical data set that would be useful to the digital forensic community through the collection and organization of 308 anti-forensic tools.

An extended classification of the original anti-forensics taxonomy, to more fully encapsulate the domain of anti-forensics.

Conclusions and future work

Future work:

Expanding the scope of the categorical data set to include more tools, of which there are many.

“Internet-of-things”: anti-forensic tools will follow this digital migration. Expand taxonomy to include the forms of digital devices that anti-forensics could exist on.

A similar methodology applied to other fields of the information assurance domain (e.g., hacking/penetration tools).

Ways of automating the classification of anti-forensic tools with computational linguistics, by parsing metadata of tools online and leveraging machine learning.

Acknowledgments

Sidharth S. Nandury and Mohammad M. Hassan

Douglas White (NIST)

Questions?

Thank you!

kconl1@unh.newhaven.edu

Data sets for this research are available at www.unhcfreg.com under *Data & Tools.*