# G-Cloud 15
# CameraForensics Site Fingerprinting Service Definition

*The service features and processes described here are accurate at the date of submission (January 2025). Any variations or upgrades will be notified as part of the order acceptance process.*

## Our Service

The disruption and prevention of the distribution of illegal harmful material on the web is hampered by challenges in identifying sites that are being used to distribute illegal content, and the fact that even when takedown efforts are successful, these sites are often quickly put back online at a different URL with small changes to their content or structure to frustrate law enforcement.

The Site Fingerprinting system crawls a list of target domains and linked sites and extracts a "fingerprint" which is collated from a range of different site characteristics. This search is seeded with initial targets that are input by users or identified during automated crawling. Having identified a list of target domains and linked sites the system compiles a fingerprint from each, which is collated from more than 20 different site characteristics. This fingerprint can then be used to identify recurrences of the same site in different locations even if that site has been superficially modified.

The extraction and analysis process to compute a site fingerprint also provides classification information that can help investigators identify new sites of interest and focus on those sites that are most likely to require action.

## Service Commitment

Our system is accessible 24/7 with an availability well in excess of 99.9% over the past 3 years. Second-line support is provided via a dedicated email account. Users and/or their first line support are able to raise issues which are responded to by email or telephone during business hours (typically within 2 hours), or if reported out of hours, at the start of the next working day.

## Accessing the Service

Our service is accessed using an up to date browser, from any location where local firewall and access control policies permit https connection. No software download or local installation is required.

The CameraForensics Firebreak user interface is efficient and intuitive, thereby minimising training requirements and making the tool suitable for infrequent use.

## Further Training and Support

Expert-lead online training sessions are available (2 included in the baseline service costs). Additional Expert or Bespoke online or on-site training can be delivered (at extra cost) to develop expert users and local champions.

## Onboarding

On receipt of a purchase order under the G-Cloud 15 Framework an appointed representative from the customer organisation will be approved to issue user account requests for employees, agents and independent contractors in their organisation. These users will have access to the full Service unless the customer representative requests withdrawal of their account, or the licence period lapses.

## Security

On request, the system can record user activity, including a timestamp for each of the various events, and details on who was logging in/searching/acting in that event. These data are available to nominated client administrator accounts. If necessary, collection of this data can be disabled to meet user security or privacy requirements. Monthly reporting, including standard metrics on the service performance against the SLA and issues raised and resolved, will be provided. This level of support is included in the baseline service costs.

## Support and Availability

Our system is accessible 24/7 with an availability well in excess of 99.9% over the past 3 years. Second-line support will be provided via a dedicated email account. Users and/or their first line support will be able to raise issues which will be responded to by email or telephone during business hours (typically within 2 hours), or if reported out of hours, at the start of the next working day.

## Offboarding

At the end of a contract period, the associated user and manager accounts are suspended. API keys are disabled. Account data can be provided and/or deleted at the customer's request. Accounts and keys can be preserved and reactivated under a new contract. Retained information includes user search histories and search parameters included in the standard audit log. The logs for a given user or organisation can be provided on request to appropriate management account holders. Data is typically provided in CSV format.

# Additional Services

We offer a range of enhancements and variations to the standard service to suit different deployments and requirements.

## 1: Customisation

Site Fingerprinting can be customised on request. This can include updates to meet new threats, application of specific techniques and integration with 3rd-party data sources and systems.

## 2: Deployments on or Integration With Customer-Specified Systems

Deployment of the system to a specified host environment, including establishing mechanisms for regular data updates and associated support.

## 3: Expert Training

Develops expert users and/or “train the trainer”. The form of the training is in-person 1 day for 25 users (customer supplies suitable room and facilities in the UK mainland). The approach will be a mix of theoretical and practical elements.

## 4: Bespoke Training

Development and delivery of a training course (either virtually or in-person) around CameraForensics Firebreak and underlying technologies, specific to customer needs.

## 5: Specific Support

Support for users around CameraForensics and underlying technologies, specific to customer needs.